PRTG Traffic Grapher 6

User Manual

Contents

Monitoring Networks With PRTG Traffic Grapher 1

Why Monitoring Of Bandwidth and Network Usage Is Important 1
What PRTG Traffic Grapher can do for you 2
PRTG Traffic Grapher Feature List 3
Base Features 3
Supported Data Acquisition Methods 3
Windows and Web Based User Interface 4
Monitoring Database 4
Internal Web Server 4
Reports 5
Notifications 5
SNMP Related Features 5
Other System Features 5
Freeware Edition and Commercial Editions 6
Ordering PRTG Traffic Grapher Commercial Editions 6
Choosing the right software - PRTG Traffic Grapher vs. IPCheck® Server Monitor 6
More about IPCheck Server Monitor 7

Installation 8

System Requirements 8
System Requirements for the Web Interface 8
System Requirements for SNMP Monitoring 8
System Requirements for NetFlow Monitoring 9
System Requirements for Packet Sniffing 9
Download 9
Downloading the Freeware Edition and Trial Edition 9
Downloading the Commercial Editions 9
Upgrading to Version 6 From Previous Versions 9
If Version 5.x is installed 9
If Version 4.x is installed 10
If Versions 1.x, 2.x, or 3.x are installed 10
Installation 10
Starting the Setup Routine 11
Walking through the installation Wizard 11
Uninstalling PRTG Traffic Grapher 14

Networking Basics You Should Be Aware Of 15

Who should read this section 15
A Short Introduction To IP Addresses 15
IP Addresses 15
IP Classes 16
SNMP Basics 17
What is SNMP? 17

SNMP Version 1, 2c and 3 17
What is an "SNMP Community String"? 18
How PRTG works with SNMP 18
SNMP uses UDP 18
SNMP, MIBs, and OIDs – an Overview 19

How to Choose A Method of Data Acquisition 20

Who should read this section 20
Available Methods of Data Acquisition 20
SNMP Monitoring 21
How SNMP Monitoring works 21
Reasons To Choose SNMP Monitoring 21
Packet Sniffing 22
How Packet Sniffing works 22
Reasons To Choose Packet Sniffing 22
NetFlow Monitoring 23
How NetFlow Monitoring works 23
Reasons To Choose NetFlow Monitoring 23
Latency Monitoring 23
How Latency Monitoring works 24
Reasons to Choose Latency Monitoring 24
Comparison of SNMP, Packet Sniffing, and NetFlow 24
How to Set Up Traffic Monitoring for Various Network Infrastructures 25
A0: Monitoring Network traffic for a single PC connected to the Internet via DSL, cable, or a modem 26
A2: Monitoring Total Network traffic with NetFlow 26
A3: Monitoring Total Network traffic using a switch with monitoring port 26
B1: Monitoring Network traffic of each PC (or connection) in a network using a switch/router with SNMP support 27
B2: Monitoring Network traffic for each PC (or connection) with NetFlow 27
B3: Monitoring Network traffic for each PC using a switch with monitoring port 27
C2: Monitoring network traffic by IP address or protocol with NetFlow 28
C3: Monitoring network traffic by IP address or protocol using a switch with monitoring port 28
D1: Monitoring Network traffic for a PC running PRTG using SNMP 29
D3: Monitoring Network traffic for a PC running PRTG using Packet Sniffing 29
E3: Monitoring Network traffic for a PC running PRTG using Packet Sniffing 29
F1: Monitoring total Network traffic of a shared Internet connection or leased line using a switch/router with SNMP support 29
G2: Monitoring network traffic by IP address or protocol of a shared Internet connection or leased line - Monitoring with NetFlow 30
G3: Monitoring network traffic by IP address or protocol of a shared Internet connection or leased line - Monitoring with Packet Sniffing 30

First Steps with PRTG Traffic Grapher 30

Basic Concepts: Understanding Views, Sensors, Graphs, Charts, Tables, and Tags 30
Views 30
Sensors 31
Graphs and Charts 32
Tables 33
Tags 34
Starting PRTG for the first time 35
Adding New Sensors using the Add Sensor Wizard 36
A First Look at The Main Window 40

Using the Windows GUI 41

Navigating Views, Sensors, Graphs, and Tags 41
PRTG's Main Window 42
Available Views 42
Data View 43
Events View 45
Sensors View 45
Custom View 45
Reports View 46
Web Browser View 47
Working With Sensors 47
Working With Charts 48
Graph Context Menu 48
Graph Details Dialog 48
Using the View Menu 51
Change Colors & Layout 51
View Historic Data 53
Compact Mode and Always On Top 53
Open Web View in Browser 54

Adding Sensors 54

Available Sensor Types 54
Adding SNMP Sensors 54
Choosing between Standard Traffic, SNMP Helper, Library, or Custom SNMP Sensors 54
All SNMP Sensor Types: Starting the Add Sensor Wizard 55
All SNMP Sensor Types: Device Selection 57
SNMP Traffic Sensors: Port Selection 58
SNMP Helper Sensors: Sensor Selection 60
OIDLIB/MIB Library Sensors: Sensor Selection 60
Custom SNMP Sensors: OID Entry 61
All SNMP Sensor Types: Additional Settings 62
Adding Packet Sniffer Sensors 63
Starting the Add Sensor Wizard 63
Filter Setup 65
Protocol Setup 67
Additional Settings 67
NetFlow Sensors 68
Setting up NetFlow Collectors 69
Starting the Add Sensor Wizard 70
Filter and Protocol Setup 72
Additional Settings 72
Adding Aggregation Sensors 73
Before you start 73
Starting the Add Sensor Wizard 73
Working with Aggregation Sensors 74
Notes and Limitations 74
Automatic Network Discovery 75

Editing Sensors 77

Identification Settings 78
Comments Settings 78
Sensor Settings 79
Advanced Settings 80

Billing Settings 80
Access Settings 81
Notifications & Limits Settings 81
Error Notifications 82
Threshold Notifications 83
Volume Notifications 83
Limit Lines 84
Common Settings for Notifications 85
Communication Settings 87
Communication Settings for SNMP Sensors 87
Communication Settings for Netflow Sensors 88
Communication Settings for Packet Sniffer Sensors 88
Filter Settings 89
Channel Settings 89
Toplists Settings 90
Editing a Toplist 91

Working with Custom Graphs 93

The Concept of Custom Panels 93
Panels 94
Working with Panels 94
Adding Panels 95
Editing Panels 97
Deleting Panels 97
Arranging Panels 97
Adding Custom Graphs and Tables to a Panel 98
Creating a New Graph 99
Creating a New Table 99
Creating a Toplist 100
Working with Graphs and Tables 100
Opening Graph's or Table's Details 100
Editing a Graph or Table 100
Deleting a Graph or Table 105

Using the Web Interface 105

Concept 105
Accessing the Web Interface 106
Basic Layout of the Web Interface 107
Header Area 108
Sensor List View 109
Custom Graphs View 110
Events View 111
Sensor Data View 112

Creating Reports 113

Reporting and Billing Concept 113
Adding Reports 113
Editing Reports 113
Settings 114
Sensors 114
Email & Export 115
Viewing Reports 116
Exporting Reports to PDF, HTML, Excel, RTF, and TIFF 117
Reading Reports 117

Graph ... 117
Detail Data ... 118
Summary and Billing Data ... 118

Setting Program Options 119

User Interface Settings ... 119
Reporting Settings ... 120
Billing Settings ... 120
How to Set up a Pricing Model ... 121
Percentile Settings ... 122
Web Server Settings ... 123
Website Settings ... 123
Web Server User Settings ... 127
Web Server Group Settings ... 127
System Settings ... 128
Mail Server Settings ... 128
Tweaks Settings ... 129
High Compatibility Mode ... 130
Advanced Port Name ... 131
Schedules Settings ... 132

Advanced Usage 133

Paessler SNMP Helper ... 133
SNMP Helper License Options ... 133
Fully Integrated Into Paessler's Monitoring Products ... 134
SNMP Helper Freeware Edition ... 134
SNMP Helper Pro Edition and its Extensions ... 134
Installing Paessler SNMP Helper ... 134
Working with Device Templates ... 136
Accessing Logfiles ... 138
Importing MIBs using Paessler MIB Importer and Converter ... 138
Editing Filter Libraries ... 139
Editing Channel Libraries ... 140
Editing the Skin of the Web GUI ... 141
Restoring Lost Sensor Settings From DAT files ... 141
Importing Configuration Files from MRTG ... 142

Appendix 142

Articles from the Paessler Knowledge Base ... 142
How to set up traffic monitoring with PRTG for various infrastructures ... 142
Configuration Tips for Cisco Routers and PRTG (NetFlow/SNMP) ... 143
Netflow 5 Filter Parameters supported by PRTG Traffic Grapher ... 143
Planning large installations of PRTG Traffic Grapher ... 143
How PRTG Traffic Grapher stores its data ... 143
Using live graphs from PRTG in other webpages using static image URLs ... 143
How to find out OIDs for PRTG's custom SNMP sensors ... 143
Upgrading from PRTG Version 3 to Version 5/6 ... 144
Why PRTG may stop recording data as soon as the Windows GUI is closed ... 144
PRTG service is not started (Event ID 7000/Error 193 in system log) ... 144
Automated License Key Installation for PRTG Traffic Grapher ... 144
What do the values in the exported CSV log file say? ... 144
Howto: Installing SNMP Service on Windows NT/2000/XP ... 144
Howto: Installing SNMP on Linux ... 145
Howto: Troubleshooting the device setup when using SNMP ... 146

Support and License **146**

Support....146
Copyright....147
Consulting and Custom Software....147
License/Usage Terms....147
Acknowledgements....152

Index Fehler! Textmarke nicht definiert.

Monitoring Networks With PRTG Traffic Grapher

Paessler Router Traffic Grapher monitors, records, and analyzes traffic data within a network, and provides accurate data about network traffic and usage trends. PRTG displays the results in various easy to read forms, and is easily customized and adapted to your needs.

Why Monitoring Of Bandwidth and Network Usage Is Important

Today most businesses rely more or less on a computer and network infrastructure. So, the computer network's reliability and speed are crucial for these businesses to be successful, as well as an efficient use of the available resources.

For the network administrator this means that he has to ensure his network's uptime, reliability, and speed – and the efficient use of the network. To do this, monitoring the network is inevitable.

PRTG Traffic Grapher monitors network and bandwidth usage as well as various other network parameters like memory and CPU usages, providing system administrators with live readings and periodical usage trends to optimize the efficiency, layout, and setup of leased lines, routers, firewalls, servers, and other network components.

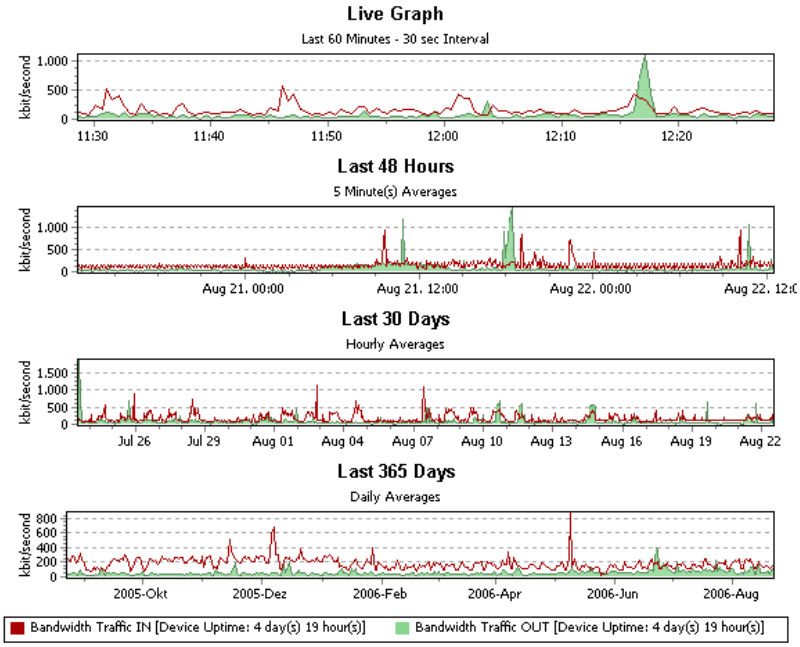
What PRTG Traffic Grapher can do for you

PRTG (Paessler Router Traffic Grapher) is an easy to use software that monitors bandwidth usage and many other network parameters via SNMP, Packet Sniffing, or Cisco NetFlow. It allows you to quickly and easily set up and run a monitoring station for networks. With just a few mouse clicks you can log the amount of data flowing through routers and leased lines, monitor CPU utilization, analyze the traffic by type, or check disk space usage.

The most common usage is monitoring the bandwidth usage of leased lines, routers, and firewalls via SNMP, packet sniffing, or NetFlow. But you can also monitor many other aspects of servers, managed switches, printers, and other network components, as long as they are SNMP enabled.

PRTG Traffic Grapher runs on a Windows machine in your network for 24 hours every day and constantly records the network usage parameters. The recorded data is stored in an internal database for later reference.

Here are two sample graphs showing the usage of a 2 MBit/s leased line over various time periods:



The recorded monitoring statistics can be viewed in the Windows GUI of PRTG Traffic Grapher. Also, all aspects of the configuration of the sensors is done using the Windows GUI.

For remote access to the monitoring results PRTG Traffic Grapher comes with a built in web server for easy access to graphs and tables using a web browser.

For data acquisition the three most common methods for bandwidth monitoring are supported:

- Using SNMP (Simple Network Management Protocol) to access traffic counters or other readings from SNMP enabled devices (most common)
- Looking at incoming/outgoing network packets that pass through a network card of a computer (so called “packet sniffing”)

- Analyzing Cisco NetFlow packets send by Cisco routers

Included with the installer is the tool “Paessler SNMP Helper (Freeware Edition)” which drastically eases accessing various system readings on Windows 2000/XP/2003 systems via SNMP which usually is very complicated. Optional Pro Editions of SNMP Helper are also available for Exchange, SQL, ISA, and Biztalk Server, see www.paessler.com/snmphelper.

PRTG Traffic Grapher is available in both a Freeware edition (limited to monitoring up to three network devices and suitable for home users and SOHOs) and several commercial editions offering monitoring for multiple network devices and advanced features needed by companies.

PRTG Traffic Grapher Feature List

PRTG Traffic Grapher makes usage monitoring for computer networks easy. Here is a list of the most important features:

Base Features

- Reliable network monitoring used by more than 100.000 users every day
- Supports data acquisition via SNMP, packet sniffing, NetFlow protocol, or latency measurement
- Classifies network traffic by IP address, protocol and other parameters
- Works with most switches, routers, firewalls, and other network devices
- Easy installation with a few clicks on Windows 2000/XP/2003
- Monitoring engine is capable of monitoring up to several thousand sensors
- A Freeware Edition is available for smaller networks
- Creates scheduled reports from the monitoring data
- Sends out alarms for failing or overloaded sensors
- Includes a built-in web server for remote access to the monitoring results

Supported Data Acquisition Methods

All common methods for network usage data acquisition are supported:

- SNMP: Simple Network Management Protocol is the basic method of gathering bandwidth and network usage data. It can be used to monitor bandwidth usage of routers and switches port-by-port as well as device readings like memory, CPU load etc.
- Packet Sniffing: The Packet Sniffer inspects all network data packets passing the PC's network card(s) and is able to classify network traffic by IP address, protocol and other parameters
- NetFlow: The NetFlow protocol is supported by most Cisco routers to measure bandwidth usage. Although being the most complex type to set

up it is also the most powerful method suitable for high traffic networks and can also classify network traffic by IP address, protocol and other parameters.

- Note: Only with Packet Sniffer and NetFlow based monitoring it is possible to measure the traffic by IP address, and/or protocol. SNMP based traffic measurement is port-based only.

Additionally you can monitor latencies using PINGs, e.g. to monitor the jitter and packet loss of a data line.

Windows and Web Based User Interface

- Monitoring data can be accessed via a Windows GUI and a web based front end
- Intuitive Windows user interface for data retrieval and configuration
- Integrated web server for remote access (no external web server necessary)
- Results are shown in various graphs and tables
  - live data for last 5-60 minutes
  - x minute average for up to 48h
  - hourly averages for up to 60 days
  - daily averages for up to 365 days
  - Top Talkers, Top Protocols, Top Connections
  - Events
- Graphs and tables are always generated on-the-fly for live reporting

Monitoring Database

- Internal database system optimized for fast and efficient storage of historic data
- Optional export of monitoring results into CSV files for custom reporting
- Database offers optional zipped backup and purging of old data

Internal Web Server

- Easy to use navigation allows to drill into the live monitoring results
- Fully "skinable" web interface using HTML templates (several default skins included)
- Web server supports public access (anyone can view the data) as well as authenticated access (username/password required) with multiple user account

Reports

- Configurable reports (graphs and data tables) in HTML, RTF, XLS, TIFF or PDF format can be created on schedule or on demand
- Reports can be exported via email or saved to file
- x% percentile calculation for any percentile value, any interval, and any time frame
- Includes a billing system for bandwidth based billing

Notifications

- For each sensor individual email notifications can be configured that notify about
  - Errors (e.g. device is not reachable)
  - Reaching traffic limits (e.g. more than x MB transferred per day or month)
  - Reaching traffic or usage thresholds (e.g. more than 700kbit bandwidth for more than one hour)

SNMP Related Features

- Monitors any value that is accessible by SNMP (i.e. any given OID Object ID)
- Supports SNMP Version Versions 1, 2c, and 3
- Supports 64 bit counters (for SNMP V2c and 3)
- Brings its own extensive OID database with many preconfigured SNMP settings (e.g. for CPU loads, disk usages, printer pagecounts, environmental monitoring, and many more)
- Supports Paessler SNMP Helper for easy access to several thousand performance counters on Windows based machines via SNMP
- MIB files can be converted into OIDLIBs to monitor any device that supports SNMP
- Various SNMP parameters (e.g. port, timeout) can be set by the user

Other System Features

- Runs as an "nt service" on Windows 2000/XP/2003 to ensure that monitoring runs all the time (you do not have to be logged into your machine to keep monitoring running)
- Extensive filtering can be applied for NetFlow and Packet Sniffing based monitoring
- MRTG configuration file import

Freeware Edition and Commercial Editions

The Freeware Edition is free for personal and commercial use. Simply download PRTG Traffic Grapher and give it a try. The Freeware Edition is limited to monitoring up to three sensors (e.g. one reading on three devices or three interfaces on one device).

If you want to monitor more devices you must purchase a commercial license. Prices start at $99.95 (€79.95) and ordering is quick and simple. If you pay online with your credit card your license key is usually delivered to your email address in a matter of minutes!

And we make ordering totally risk-free with our 30-day Money-Back Guarantee!

Ordering PRTG Traffic Grapher Commercial Editions

PRTG Traffic Grapher is developed and sold by

Paessler AG
Hornschuchpromande 7
90762 Fuerth (Germany)
Fax: +49-911-7399031

To order licenses please visit our website:
http://www.paessler.com/order

To contact our sales department send an email to sales@paessler.com.

You can order online, by fax or by purchase order.

Choosing the right software - PRTG Traffic Grapher vs. IPCheck® Server Monitor

While PRTG is specialized in bandwidth and traffic monitoring (but also monitors any other value accessible by SNMP) its sister product IPCheck Server Monitor is more specialized in monitoring uptimes/downtimes and notifying the administrators in case of failures.

Since both products can do some similar tasks the following matrix will help you to choose the right software:

	PRTG® Traffic Grapher	IPCheck® Server Monitor
Monitoring bandwidth usage using SNMP	**specialized**	only basic functionality
Monitoring various network parameters using SNMP (e.g. CPU Loads, disk usage, temperatures)	Yes	Yes
Analyzing network packets passing through local network cards	**Yes**	No
Analyzing Cisco NetFlow data streams	**Yes**	No

Monitoring network for uptimes and downtimes	only basic functionality	**specialized**
Monitoring any OID value	Yes	Yes
Sending notifications for slow or failing devices, downtimes, etc.	only email, EXE/BAT file execution and HTTP Request	**Lots of options** (configuration of delays, notifications via email, ICQ, SMS, Pager, HTTP, NETSEND, etc.)
Daily Reports via email	Yes	Yes
Daily/Monthly bandwidth usage reports and billing system	**Yes**	No
Number of sensors that can be monitored simultaneously	Hundreds and thousands	Hundreds and thousands
Runs on Windows	2000, XP, 2003	NT, 2000, XP, 2003
Type of remote access	Built-in web-server	Built-in web-server
Freeware Edition or Free Trial available?	Yes	Yes
X% percentile calculation	**Yes**	No

More about IPCheck Server Monitor

This Windows-based software makes it easy and affordable to detect network and website failures early, minimizing downtime and avoiding economic impact. IPCheck Server Monitor helps organizations monitor critical network resources and immediately detect system failures or performance problems.

Here is a short list of features

- Reliable monitoring using Paessler's IPCheck™ Technology
- Fast and easy installation
- Runs as a server software on Windows 2000, XP, and 2003
- Complete and intuitive web based interface that is easy to access using a standard web browser
- Includes free SQL server for fast and reliable data storage
- Sensor types include PING, PORT, HTTP, HTTPS, Advanced HTTP, HTTP Transaction, DNS, SMTP, POP3, SNMP, SQL Servers, Windows System Sensors, and various custom sensors (i.e. user can create his own sensors using scripting and many programming languages)
- Notifications can be triggered by uptimes, downtimes, or slow responses
- Notifications sent to you by email and ICQ, via SMS, and to pagers
- Monitoring reports sent to your mailbox daily, weekly, or monthly
- Detailed reports and graphs can be viewed online

To learn more about IPCheck Server Monitor please check out:

http://www.paessler.com/ipcheck

Installation

System Requirements

Version 6 of PRTG Traffic Grapher works on the following operating systems

- Windows 2000, XP, and 2003
  - 32bit versions: fully supported
  - 64bit versions: fully supported
- Microsoft Vista and Microsoft Longhorn will be supported as soon as the final releases become available
- PRTG was tested to work fine on Windows 98 and ME, but we do not officially support these operating systems for commercial use

The following basic system configuration is required:

- 64 MB RAM (256 MB and more recommended)
- 20 MB disk space for installation
- between 25kb and 300kb disk space per sensor per day for the monitoring data database
- TCP/IP Network Connection

Please also refer to the section "Planning large installations of PRTG Traffic Grapher" if you plan an installation with more than some 50-100 sensors.

System Requirements for the Web Interface

To access the web interface of PRTG Traffic Grapher one of the following web browsers is required (others may also work but have not been tested):

- Internet Explorer 6.0 or later
- FireFox 1.0 or later

System Requirements for SNMP Monitoring

The monitored device(s) must be equipped with SNMP Version 1, 2c or 3 (i.e. an SNMP compatible software must be installed on the device). SNMP must be enabled on the device and the machine running PRTG must be allowed access to the SNMP interface.

System Requirements for NetFlow Monitoring

The device must be configured to send NetFlow data packets (NetFlow Version 5) to the machine running PRTG and a NetFlow Collector must be set up in PRTG.

System Requirements for Packet Sniffing

Only data packets passing the local machine's network card can be analyzed. For network-wide monitoring in switched networks the use of switches with so-called "monitoring ports" is necessary.

Download

Please download the latest version of PRTG Traffic Grapher from the Paessler Website.

There are two different installers for PRTG, a public download for the Freeware and Trial Editions, and another download for the Commercial Editions (which is only available for paying customers).

Downloading the Freeware Edition and Trial Edition

Please download the latest publicly available files from the Paessler website, www.paessler.com/prtg/download

Downloading the Commercial Editions

Upgrades are free to customers with active maintenance contract. Please log into the Paessler website at www.paessler.com/login to request the latest download.

If you do not have an active maintenance contract please contact sales@paessler.com.

Upgrading to Version 6 From Previous Versions

If Version 5.x is installed

Simply run the V6 installer to upgrade your version 5 installation. It will automatically overwrite the files of version with the new files and upgrade your data.

When upgrading from Version 5 to Version 6 of PRTG Traffic Grapher please keep the following points in mind:

- As usual for any software installation it is strongly recommended to create a backup of your data (i.e. the "*.prtg" file and your monitoring database) before proceeding with the installation. These files are usually stored in the following folder.

  ```
  C:\Documents and Settings\All
  Users\Documents\PRTG Traffic Grapher
  ```

- You can optionally uninstall version 5 manually before upgrading. The uninstaller will only remove the software, all your data and settings will remain untouched on the disk.
- Your sensor settings and the historic monitoring data will be automatically loaded & converted as soon as you start version 6 for the first time.
- After running version 6 once you can not go back to version 5 because the file formats are not backward compatible.

If Version 4.x is installed

Version 4 must be uninstalled before version 6 can be installed. Historic monitoring data will be preserved and automatically loaded as soon as you start version 6 for the first time.

When upgrading from Version 4 to Version 6 of PRTG Traffic Grapher please keep the following points in mind:

- After uninstalling Version 4 simply run the standard setup process of Version 6 as described in the previous section.
- As usual for any software installations it is strongly recommended to create a backup of your data (i.e. the "*.prtg" file and your monitoring database) before proceeding with the installation. These files are usually stored in the following folder.

  ```
  C:\Documents and Settings\All
  Users\Documents\PRTG Traffic Grapher
  ```

- Version 4 must be uninstalled before Version 6 can be installed. The uninstaller will only remove the software, all your data and settings will remain untouched on the disk.
- Your sensor settings and the historic monitoring data will be automatically loaded & converted as soon as you start version 6 for the first time.
- After running version 6 once you can not go back to version 4 because the file formats are not backward compatible.
- If you are using panel based authentication in the web server please check the converted new web server user accounts after upgrading.
- Since the reporting system was completely changed, the V4 email reports are not supported anymore and you must create new reports.

If Versions 1.x, 2.x, or 3.x are installed

There is no direct upgrade path for older installations (before version 4) to version 6. There is an article in the Paessler knowledge base that explains what you can do.

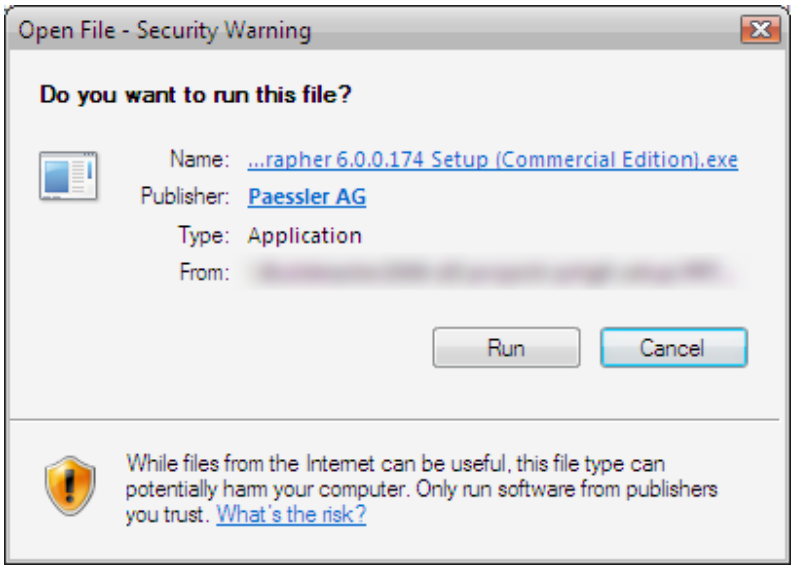
Installation

Installing the software is similar to other Windows-based applications.

Starting the Setup Routine

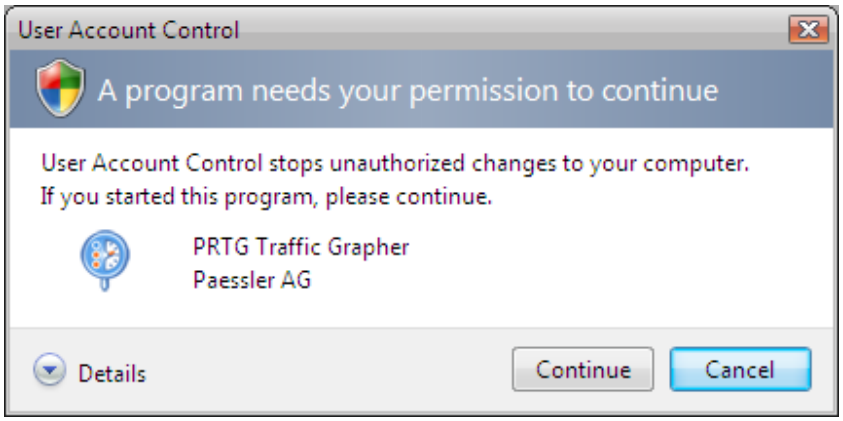
To install the application please insert your PRTG Traffic Grapher CD-ROM into your computer or open the installation setup routine from the ZIP file that you have downloaded.

On Windows XP, 2003, Vista and later operating systems you may see a security information screen like this:


Open File - Security Warning
Do you want to run this file?
Name: ...rapher 6.0.0.174 Setup (Commercial Edition).exe
Publisher: Paessler AG
Type: Application
From:
Run
Cancel
While files from the Internet can be useful, this file type can potentially harm your computer. Only run software from publishers you trust. What's the risk?

Your computer has just checked the downloaded file (e.g. to make sure it has not been tampered by a malicious software). If this dialog says "Publisher: Paessler AG" you can be sure that you are about to install the original files from the vendor.

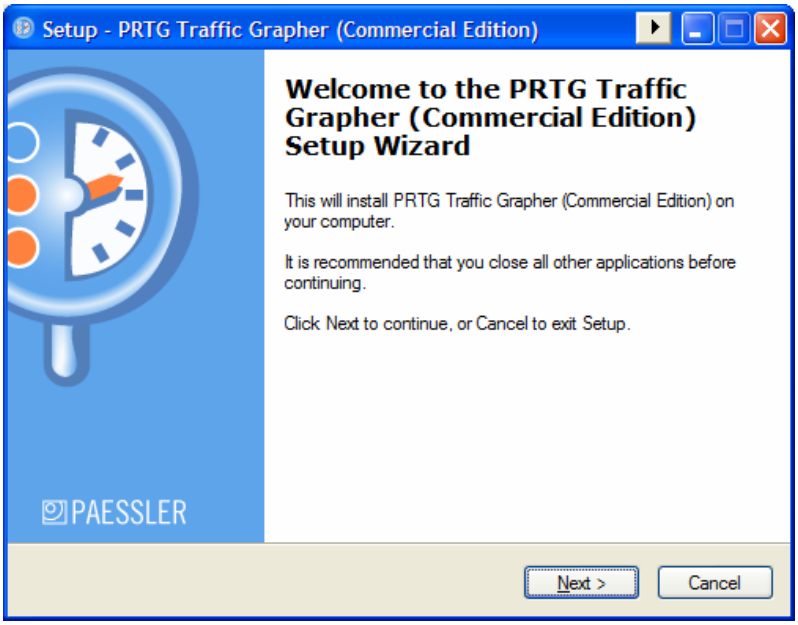
On Windows Vista you will now see another notification which tells you that a setup program has been started. Please click on **Continue**.



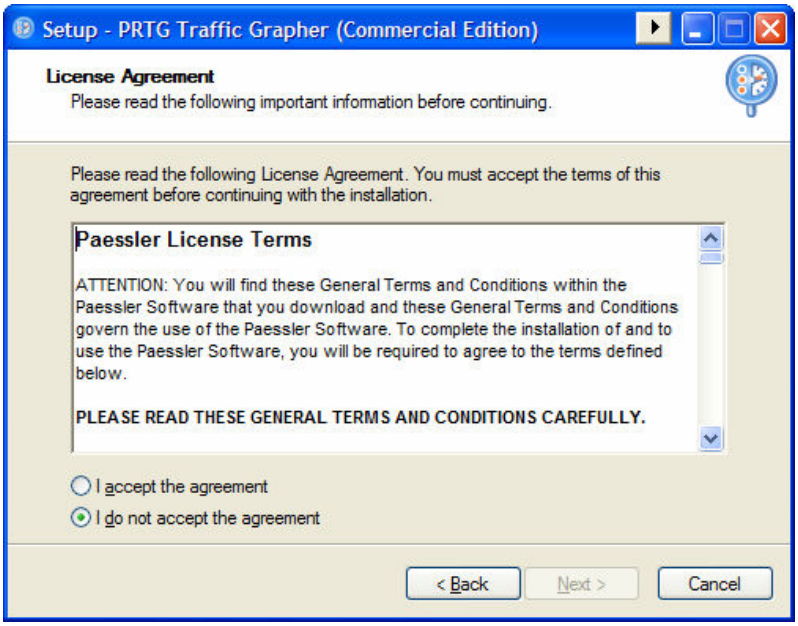
If you are installing an upgrade of PRTG you may see a notice that the PRTG Service is currently running. Please click **Yes** in order to continue the setup process.

Walking through the installation Wizard

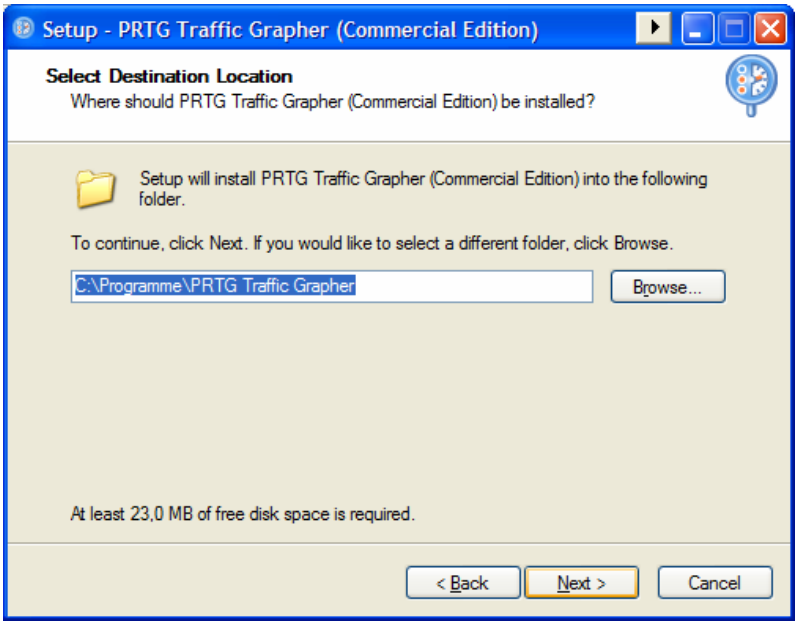
- The **Installation Wizard Welcome Screen** will show up.


Setup - PRTG Traffic Grapher (Commercial Edition)
Welcome to the PRTG Traffic Grapher (Commercial Edition) Setup Wizard
This will install PRTG Traffic Grapher (Commercial Edition) on your computer.
It is recommended that you close all other applications before continuing.
Click Next to continue, or Cancel to exit Setup.
PAESSLER
Next >
Cancel

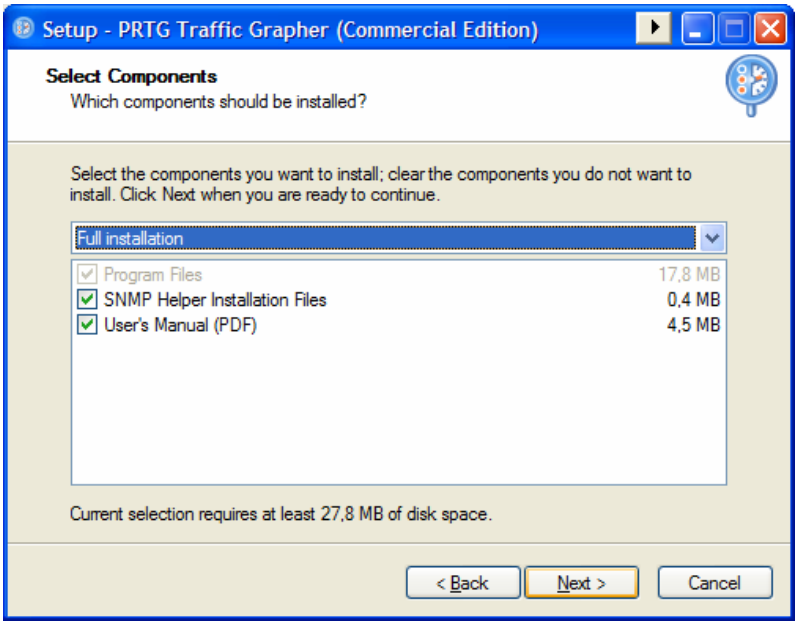
- Please click **Next** and you will be shown the license agreement.


Setup - PRTG Traffic Grapher (Commercial Edition)
License Agreement
Please read the following important information before continuing.
Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.
Paessler License Terms
ATTENTION: You will find these General Terms and Conditions within the Paessler Software that you download and these General Terms and Conditions govern the use of the Paessler Software. To complete the installation of and to use the Paessler Software, you will be required to agree to the terms defined below.
PLEASE READ THESE GENERAL TERMS AND CONDITIONS CAREFULLY.
I accept the agreement
I do not accept the agreement
< Back
Next >
Cancel

- You must accept this agreement to install the software!
- Then, click **Next** to continue. This opens the **Select Destination Window**:

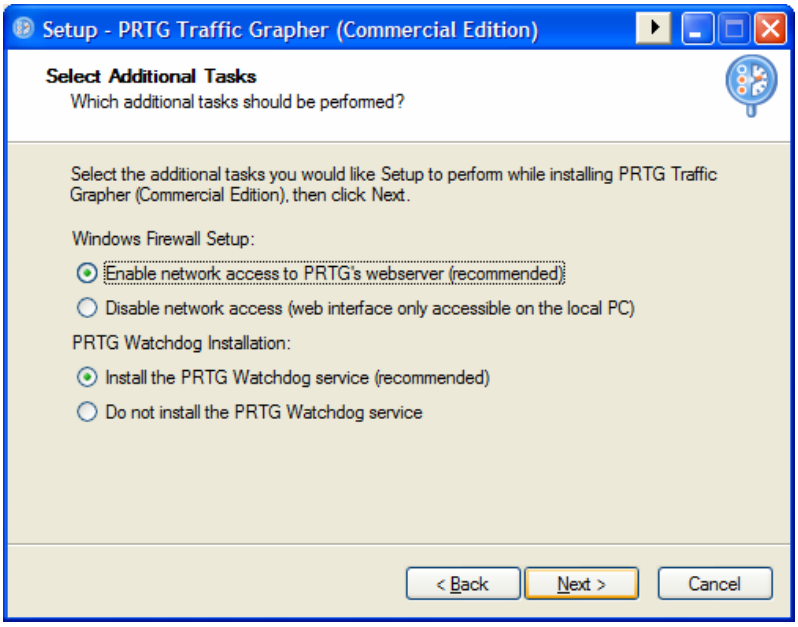

Setup - PRTG Traffic Grapher (Commercial Edition)
Select Destination Location
Where should PRTG Traffic Grapher (Commercial Edition) be installed?
Setup will install PRTG Traffic Grapher (Commercial Edition) into the following folder.
To continue, click Next. If you would like to select a different folder, click Browse.
C:\Programme\PRTG Traffic Grapher
Browse...
At least 23,0 MB of free disk space is required.
< Back
Next >
Cancel

- The **Select Destination Window** allows you to install PRTG Traffic Grapher at the default location (C:\Program Files\PRTG Traffic Grapher) or allows you to choose another location from the list. When you have selected a destination, click the **Next Button.** This will bring up the **Select Additional Tasks Window.**
- Note: When installing for the first time selecting a location other than the default location will not interfere with the program's operation. If you install an update (of the same major version number) you MUST select the same location as for the initial installation. Accepting the default is strongly recommended!


Setup - PRTG Traffic Grapher (Commercial Edition)
Select Components
Which components should be installed?
Select the components you want to install; clear the components you do not want to install. Click Next when you are ready to continue.
Full installation
Program Files 17,8 MB
SNMP Helper Installation Files 0,4 MB
User's Manual (PDF) 4,5 MB
Current selection requires at least 27,8 MB of disk space.
< Back
Next >
Cancel

- The **Select Components** window allows you to select which elements to install with PRTG.

- The SNMP Helper Installation files can be used to install this helper utility on machines you want to monitor (see the Paessler SNMP Helper section for more information)
- Click **Next** to continue. This opens the **Select Additional Tasks Window**:


Setup - PRTG Traffic Grapher (Commercial Edition)
Select Additional Tasks
Which additional tasks should be performed?
Select the additional tasks you would like Setup to perform while installing PRTG Traffic Grapher (Commercial Edition), then click Next.
Windows Firewall Setup:
Enable network access to PRTG's webserver (recommended)
Disable network access (web interface only accessible on the local PC)
PRTG Watchdog Installation:
Install the PRTG Watchdog service (recommended)
Do not install the PRTG Watchdog service
< Back
Next >
Cancel

- The **Select Additional Tasks Window** allows you to Enable or Disable the access to PRTG's web server in the Windows Firewall. You must enable this configuration to access the monitoring results in the web interface from a remote computer. If you do not choose to enable this configuration here you must later add the necessary firewall exception in the Windows Firewall settings manually.
- You can also choose to install the PRTG Watchdog service (recommended) which restarts the PRTG service in case you forget to start it manually or in case of an unrecoverable failure.
- The **Installation Window** displays PRTG Traffic Grapher's installation progress. After installation you can optionally start the program immediately.

When the installation is complete the computer may ask you to restart the machine to finish the installation. Although you can choose to reboot later, it is strongly recommended to reboot the machine right now to fully complete the installation!

Uninstalling PRTG Traffic Grapher

To uninstall PRTG Traffic Grapher:

- On your computer go to your **Control Panel.**
- Select the **Add/Remove Programs** option. This will open the **Add/Remove Programs Window**.
- Select **PRTG Traffic Grapher** from the list of programs.

- Click the **Remove button** to uninstall the program.

Or select the Uninstall icon from the PRTG Traffic Grapher group in the **Start|Programs** menu.

Note: During Uninstallation your monitoring data will not automatically be removed!

After the uninstallation of the software has finished please check PRTG Traffic Grapher's installation folder and delete all remaining files that you do not want to preserve. Also, please check the "\Documents and Settings\All Users\Common Documents\PRTG Traffic Grapher" folder for remaining data files which are also not automatically removed!

Networking Basics You Should Be Aware Of

Who should read this section

If you are new to network administration and network monitoring, read about the technical basics in this section! It will help you to understand how PRTG Traffic Grapher works!

If you are already used to IP addresses and the SNMP protocol you can skip this section.

A Short Introduction To IP Addresses

IP Addresses

In order for systems to locate each other in a distributed environment, nodes are given explicit addresses that uniquely identify the particular network the system is on and uniquely identify the system to that particular network. When these two identifiers are combined, the result is a globally-unique address.

This address, known as "IP address", as "IP number", or merely as "IP" is a code made up of numbers separated by three dots that identifies a particular computer on the Internet. These addresses are actually 32-bit binary numbers, consisting of the two sub addresses (identifiers) mentioned above which, respectively, identify the network and the host to the network, with an imaginary boundary separating the two.

An IP address is, as such, generally shown as 4 octets of numbers from 0-255 represented in decimal form instead of binary form.

For example, the address 168.212.226.204 represents the 32-bit binary number 10101000.11010100.11100010.11001100.

The binary number is important because that will determine which class of network the IP address belongs to. The Class of the address determines which part belongs to the network address and which part belongs to the node address (see IP address Classes further on).

The location of the boundary between the network and host portions of an IP address is determined through the use of a subnet mask. This is another 32-bit binary number which acts like a filter when it is applied to the 32-bit IP address. By comparing a subnet mask with an IP address, systems can determine which portion of the IP address relates to the network and which portion relates to the host. Anywhere the subnet mask has a bit set to "1", the underlying bit in the IP address is part of the network address. Anywhere the subnet mask is set to "0", the related bit in the IP address is part of the host address.

The size of a network is a function of the number of bits used to identify the host portion of the address. If a subnet mask shows that 8 bits are used for the host portion of the address block, a maximum of 256 host addresses are available for that specific network. If a subnet mask shows that 16 bits are used for the host portion of the address block, a maximum of 65,536 possible host addresses are available for use on that network.

An Internet Service Provider (ISP) will generally assign either a static IP address (always the same) or a dynamic address (changes every time one logs on).

ISPs and organizations usually apply to the InterNIC for a range of IP addresses so that all clients have similar addresses.

There are about 4.3 billion IP addresses. The class-based, legacy addressing scheme places heavy restrictions on the distribution of these addresses.

TCP/IP networks are inherently router-based, and it takes much less overhead to keep track of a few networks than millions of them.

IP Classes

Class A addresses always have the first bit of their IP addresses set to "0". Since Class A networks have an 8-bit network mask, the use of a leading zero leaves only 7 bits for the network portion of the address, allowing for a maximum of 128 possible network numbers, ranging from 0.0.0.0 – 127.0.0.0. Number 127.x.x.x is reserved for loopback, used for internal testing on the local machine.

Class B addresses always have the first bit set to "1" and their second bit set to "0". Since Class B addresses have a 16-bit network mask, the use of a leading "10" bit-pattern leaves 14 bits for the network portion of the address, allowing for a maximum of 16,384 networks, ranging from 128.0.0.0 – 181.255.0.0.

Class C addresses have their first two bits set to "1" and their third bit set to "0". Since Class C addresses have a 24-bit network mask, this leaves 21 bits for the network portion of the address, allowing for a maximum of 2,097,152 network addresses, ranging from 192.0.0.0 – 223.255.255.0.

Class D addresses are used for multicasting applications. Class D addresses have their first three bits set to "1" and their fourth bit set to "0". Class D addresses are 32-bit network addresses, meaning that all the values within the range of 224.0.0.0 – 239.255.255.255 are used to uniquely identify multicast groups. There are no host

addresses within the Class D address space, since all the hosts within a group share the group's IP address for receiver purposes.

Class E addresses are defined as experimental and are reserved for future testing purposes. They have never been documented or utilized in a standard way.

The Paessler network monitoring products PRTG Traffic Grapher and IPCheck Server Monitor use the IP address in order to connect to the respective machines they are intended to monitor / graph.

SNMP Basics

What is SNMP?

SNMP is short for "Simple Network Management Protocol". It is a set of several protocol definitions for managing networks. There are several versions of this protocol, the first versions of SNMP were developed in the early 80s.

SNMP works by sending messages (requests) to some device of a network which sends back the requested information. The requesting machine specifies the desired value with an OID (Object IDentifier) which, for example, can look like this:

```
1.3.6.1.2.1.25.3.3.1.2.2
```

Relax, for most uses of PRTG Traffic Grapher you don't need to handle any OIDs, PRTG Traffic Grapher has the most common ones stored inside the product. You will have to enter a specific OID into the program for special tasks only.

These OIDs are usually taken out of so called MIBs (Management Information Bases) which are published by the hardware manufacturers, because the OIDs often vary from one device to another.

E.g. there are OIDs for CPU usage, available disk space, transferred bytes over a network port, printed pages of a printer, and some devices even offer the room temperature as a value for environmental monitoring.

SNMP Version 1, 2c and 3

PRTG supports three versions of the SNMP protocol:

- **SNMP Version 1:** The oldest and most basic version of SNMP
  - Pros: Supported by most devices that are SNMP compatible; simple to set up
  - Cons: Limited security as it only uses a simple password ("community string") and data is sent in clear text (unencrypted); should only be used inside LANs behind firewalls, not in WANs; only supports 32bit counters which is not enough for bandwidth monitoring with high loads of some gigabits/second
- **SNMP Version 2c:** Adds 64 bit counters
  - Pros: Supports 64 bit counters to monitor bandwidth usage in networks with gigabits/second loads
  - Cons: Limited security (same situation as with SNMP V1)
- **SNMP Version 3:** Adds authentication and encryption

- Pros: Offers user accounts and authentication for multiple users and optional encryption of the data packets, which makes it much more secure; plus all advantages of Version 2c
- Cons: none

It is important to know that if you select an SNMP version which is not supported by the server or device that you want to monitor you will receive an error message. Unfortunately most of the time these error messages are not explicitly telling you about the incorrect SNMP version (they say only something like “cannot connect” or similar). The same situation exists if community string, usernames and passwords are incorrect.

What is an “SNMP Community String”?

The “SNMP Community string” is like a user id or password that allows access to a router's or other device's statistics. PRTG sends the community string along with all SNMP requests. If the community string is correct, the device responds with the requested information. If the community string is incorrect, the device simply discards the request and does not respond.

Note: SNMP Community strings are used only by devices which support SNMPv1 and SNMPv2c protocol. SNMPv3 uses username/password authentication, along with an encryption key.

By convention, most SNMPv1-v2c equipment ships from the factory with a read-only community string set to "public". It is standard practice for network managers to change all the community strings to customized values in the device setup.

How PRTG works with SNMP

For **traffic and bandwidth monitoring** PRTG Traffic Grapher logs the amount of data flowing in and out of an SNMP (see above) enabled network component. To do this PRTG Traffic Grapher constantly reads the traffic counters (Internet MIB-2) from the device.

To **monitor other SNMP values** PRTG Traffic Grapher reads the current values from the device using an OID from its own OID library or by using an OID entered by the user.

PRTG Traffic Grapher keeps track of the historic monitoring data in its database

SNMP uses UDP

UDP stands for User Datagram Protocol and is the opposite of TCP (Transmission Control Protocol).

User Datagram Protocol (defined by RFC 768) is very low overhead, fast and unreliable while TCP is a very reliable and high overhead protocol.

The unreliability comes in the form of checks and balances whereas if TCP sends something, it waits for an acknowledgment and if it doesn’t hear back, it will resend.

Since logging of devices usually happens within a time period that is cyclic in nature, it’s common sense that you missed the event and you’ll catch it next time… the tradeoff being that the low overhead protocol is simple to use and doesn’t eat up all your bandwidth like TCP based applications going across your WAN.

SNMP, MIBs, and OIDs – an Overview

SNMP stands for Simple Network Management Protocol and consists of three key components: managed devices, agents, and network-management systems (NMSs). A managed device is a node that has an SNMP agent and resides on a managed network. These devices can be routers and access server, switches and bridges, hubs, computer hosts, or printers. An agent is a software module residing within a device. This agent translates information into a compatible format with SNMP. An NMS runs monitoring applications. They provide the bulk of processing and memory resources required for network management.

MIB stands for Management Information Base and is a collection of information organized hierarchically. These are accessed using a protocol such as SNMP. There are two types of MIBs: scalar and tabular. Scalar objects define a single object instance whereas tabular objects define multiple related object instances grouped in MIB tables.

OIDs or Object Identifiers uniquely identify managed objects in a MIB hierarchy. This can be depicted as a tree, the levels of which are assigned by different organizations. Top level MIB object IDs (OIDs) belong to different standard organizations. Vendors define private branches including managed objects for their own products.

SNMP version 1was the initial development of the SNMP protocol. A description can be found in Request for Comments (RFC) 1157 and it functions within the specification of the Structure of Management Information (SMI). It operates over User Datagram Protocol (UDP), Internet Protocol (IP), OSI Connectionless Network Services (CLNS), AppleTalk Datagram Delivery Prtocol (DDP), and Novell Internet Packet Exchange (IPX). SNMP v1 is considered the de facto network management protocol in the Internet community.

SNMP works on the basis that network management systems send out a request and the managed devices return a response. This is implemented using one of four operations: Get, GetNext, Set, and Trap. SNMP messages consist of a header and a PDU (protocol data units). The headers consist of the SNMP version number and the community name. The community name is used as a form of security in SNMP. The PDU depends on the type of message that is being sent. The Get, GetNext, and Set, as well as the response PDU, consist of PDU type, Request ID, Error status, Error index and Object/variable fields. The Trap consist of Enterprise, Agent, Agent address, Generic trap type, Specific trap code, Timestamp and Object/Value fields.

MIBs are a collection of definitions which define the properties of the managed object within the device to be managed (such as a router, switch, etc.) Each managed device keeps a database of values for each of the definitions written in the MIB. As such, it is not actually database but implementation dependant. Each vendor of SNMP equipment has an exclusive section of the MIB tree structure under their control.

Using the Paessler MIB Importer you can convert MIB files into OIDLIB files which PRTG can use to create sensors.

In order for all of this to be properly organized, all of the manageable features of all products (from each vendor) are arranged in this tree. Each “branch” of this tree has a number and a name, and the complete path from the top of the tree down to the point of interest forms the name of that point. This is the OID. Nodes near the top of the tree are extremely general in nature. For example, to get to the Internet, one has to reach to the fourth tier. As one moves further down, the names get more and more specific, until one gets to the bottom, where each node represents a particular feature on a specific device (or agent).

Here is a sample structure of an OID:

Iso (1).org(3).dod(6).internet(1).private(4).transition(868).products(2).chassis(4).card(1).slotCps(2)-.-cpsSlotSummary(1).cpsModuleTable(1).cpsModuleEntry(1).cpsModuleModel(3).3562.3

or

1.3.6.1.4.868.2.4.1.2.1.1.1.3.3562.3

These numbers are the ones used in PRTG when setting up custom sensors, in order to access the appropriate elements of the device desired to be monitored. OIDs are generally provided by the hardware manufacturers or can be found in so-called OID repositories, where collections of MIB trees and the respective OIDs can be accessed. PRTG reads these OIDs and appoints them to the pertinent device, respectively monitoring the selected device and its OID specific.

How to Choose A Method of Data Acquisition

Who should read this section

This section explains the available methods of data acquisition. It is strongly recommended to all users to read this section as it will help you to understand how the program works!

Available Methods of Data Acquisition

Depending on your infrastructure you can monitor the usage of your network using different methods supported by PRTG Traffic Grapher.

You can choose between four common methods for (bandwidth) monitoring:

- SNMP: Using SNMP (Simple Network Management Protocol) to access traffic counters or other readings from SNMP enabled devices (most common)
- Sniffing: Looking at incoming/outgoing network packets that pass through a network card of a computer (so called packet sniffing)
- NetFlow: Analyzing Cisco NetFlow packets sent by Cisco routers

- Latency: Monitoring performance of a data line or a device by measuring PING times

Depending on your network configuration and your monitoring needs you must choose between these methods. All methods can be used at the some time, too.

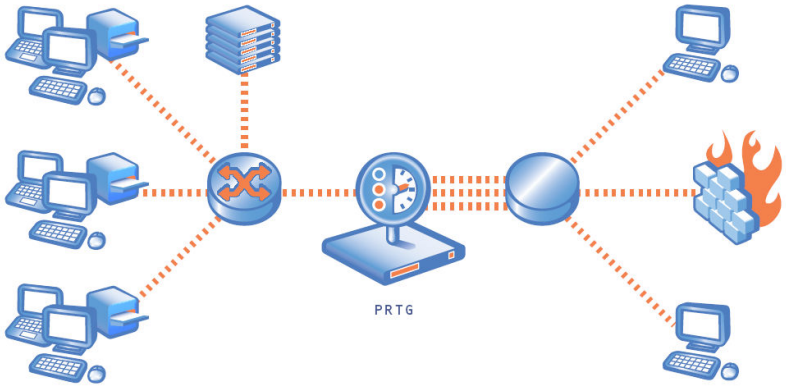
Please read on to understand the differences between the four methods.

SNMP Monitoring

The Simple Network Management Protocol (SNMP) is the most basic method of gathering bandwidth and network usage data.

How SNMP Monitoring works

It can be used to monitor bandwidth usage of routers and switches on a port-by-port basis, as well as device readings like memory, CPU load, etc.



When this technology is used PRTG queries the devices (e.g. routers, switches, and servers) for the traffic counters of each port with quite small data packets. These packets are triggering reply packets from the device. This option creates the least CPU load and network load of the three methods.

Reasons To Choose SNMP Monitoring

SNMP is the most commonly used method mainly because it is easy to set up and requires only minimal bandwidth and CPU cycles.

So if your network devices support SNMP and/or if you want monitor large networks with several hundred sensors we recommend to get started with SNMP.

Besides network usage monitoring one unique feature of SNMP is the possibility to also monitor other network parameters like CPU loads, disk usage, temperatures, as well as many other readings (depending on the device). This is only possible using SNMP.

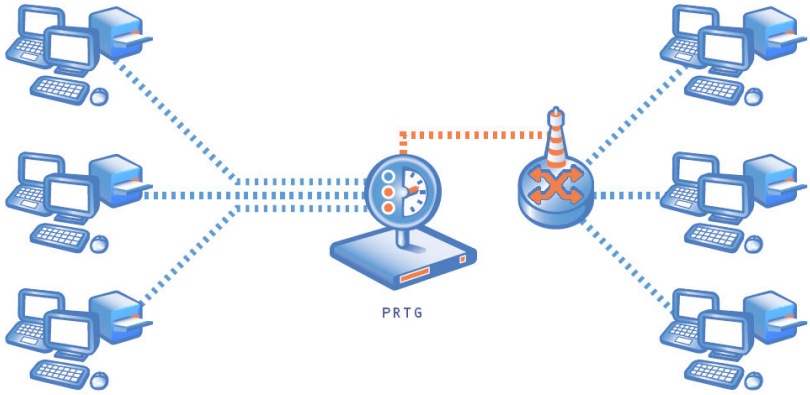
Network issues: In order to use SNMP for monitoring it must be possible for UDP packets to travel from the machine running PRTG to the device you want to monitor and back, which is usually the case in LANs and Intranets. For Internet Connections, DMZ, and WAN connections this is usually not the case and some changes to the traversed firewalls may be necessary. Keep in mind that SNMP V1 and V2c are not secure protocols and should not be used across the Internet. Only SNMP version 3 supports encryption.

Packet Sniffing

Packet Sniffing comes into consideration if your network device(s) do not support SNMP or if you need the differentiation of the bandwidth usage by network protocol and/or IP addresses.

How Packet Sniffing works

If you need to know what applications or IP-addresses are causing the traffic in your network you can use a Packet Sniffer which looks at every single data packet traveling in your network for accounting purposes.



PRTG can analyze the packets passing the network card of a PC or it can be connected to a so-called monitoring port of a switch.

In order to calculate bandwidth usage PRTG inspects all network data packets either passing the PC's network card (shown on the left side) or the data packets sent by a monitoring port of a switch (right side) with its built-in Packet Sniffer.

From the three bandwidth monitoring technologies this one creates the most CPU and network load and thus should only be used in small to medium networks or for individual computers.

Reasons To Choose Packet Sniffing

It is important to understand that the packet sniffer can only access and inspect data packets that actually flow through the network interface(s) of the machine running the PRTG software.

This is fine if you only want to monitor the traffic of this machine (e.g. your web server). But in switched networks only the traffic for a specific machine is send to each machine's network card, so PRTG can usually not see all the traffic of the other machines in the network.

If you also want to monitor the traffic of other devices in your network you must use a switch that offers a "monitoring port" or "port mirroring" configuration (Cisco calls it "SPAN").

In this case the switch sends a copy of all data packets traveling through the switch to the monitoring port. As soon as you connect the machine that runs PRTG to the monitoring port the packet sniffer is able to analyze the complete traffic that passes through the switch.

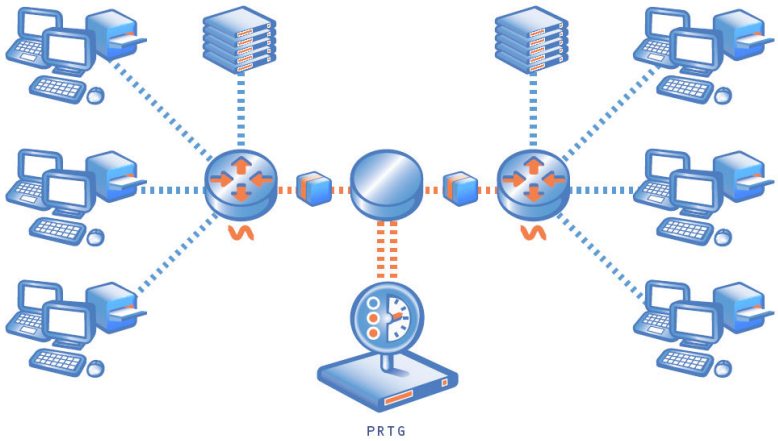
Another option is to use the PC running PRTG Traffic Grapher as a gateway for all the other computers.

NetFlow Monitoring

NetFlow monitoring is the domain of networks that use Cisco switches.

How NetFlow Monitoring works

One option to measure bandwidth usage "by IP address" or "by application" is to use Cisco's NetFlow protocol which is especially suited for high traffic networks. Many routers and switches from Cisco support this protocol.



Cisco devices with NetFlow support track the bandwidth usage of the network internally and then only send pre-aggregated data to the PRTG system for accounting purposes. This way the computing load for PRTG is much lower. This option is recommended for high traffic networks.

Reasons To Choose NetFlow Monitoring

NetFlow monitoring is the domain of networks that use Cisco switches. These switches can be configured to sent data streams with the network's usage data to the machine running PRTG which can then analyze the data.

Because the switch already performs a pre-aggregation of traffic data the flow of data to PRTG is much smaller than the monitored traffic. This makes NetFlow the ideal option for high traffic networks that need differentiation of the bandwidth usage by network protocol and/or IP addresses.

Latency Monitoring

The option to monitor latencies was added to PRTG so the user is able to monitor the performance of a data line.

How Latency Monitoring works

In order to perform latency monitoring PRTG sends an "ICMP echo request" (also known as PING) to the device and records the time it takes to receive the answer ("ICMP echo answer").

Reasons to Choose Latency Monitoring

A high variation of PING times on a data line (so-called "jitter") can be a sign of an overloaded device or data line. A well performing data line should show an almost steady value.

Too many lost PINGs ("packet loss") is also a sign of an overloaded network device.

Comparison of SNMP, Packet Sniffing, and NetFlow

The following table shows the differences between the three methods that can be used for Bandwidth Monitoring:

	SNMP	**Packet Sniffing**	**Netflow**
Setup	Easy	Easy to Complex (depending on filter rules used)	Can be complex (e.g. the switch must be configured)
Traffic can be filtered	No	Yes	Yes
Differentiate bandwidth usage by protocol or IPs	No	Yes	Yes
PRTG can show Toplists (Top Talker, Top Connections, Top Protocols, etc.)	No	Yes	Yes
Filter bandwidth usage by IP	No	Yes	Yes
Filter bandwidth usage by MAC address	No	Yes	No
Filter bandwidth usage by physical network port	Yes	No	No
Monitor network parameters other than bandwidth usage	Yes	No	No
CPU load on the machine running PRTG	Low	Higher, depends on the amount of traffic	Higher, depends on the amount of traffic
Excess bandwidth usage of monitoring	Small	None (except when monitoring switch ports are used)	Depends on the traffic

How to Set Up Traffic Monitoring for Various Network Infrastructures

This section explains the various options you have to monitor the network traffic that occurs inside LANs or that goes over a shared Internet connection or leased line.

With PRTG's data acquisition technologies and the various infrastructure options in use today it can sometimes get complicated to decide which monitoring technology is right for your problem.

The easiest configuration is to monitor the local traffic of one PC by installing PRTG directly on it. This scenario is used to monitor a single PC in a LAN network or to monitor a PC connected to the Internet via DSL, modem, or cable (see: A0).

For other network configurations use the following table to find your situation or task and follow the corresponding instructions below:

Step 1: Select Your LAN infrastructure				
	Network switch, router or other device with SNMP support	Router with Netflow support	Managed switch with monitoring port option (or a hub)	Unmanaged switch or router
	Technology: SNMP	Technology: NETFLOW	Technology: Packet Sniffing	Technology: Packet Sniffing
Step 2: Choose what to monitor:				
Option I: Centralized LAN Traffic Monitoring				
Total Network Traffic	O	A2	A3	O
Traffic per PC	B1	B2	B3	O
Traffic per IP or protocol	O	C2	C3	O
Option II: Monitoring just one PC on which PRTG runs on				
Traffic of local PC	D1	O	D3	
Traffic per IP or protocol	O	O	E3	
Option III: Monitoring usage of a shared Internet connection or leased line				
Total Leased Line Traffic	F1	O	O	O
Traffic per PC, IP or protocol	O	G2	G3	O

A0: Monitoring Network traffic for a single PC connected to the Internet via DSL, cable, or a modem

- Simply create one new Packet Sniffer sensor and select the PC's network card during the "Add Sensor" wizard and you will get the total network traffic
- If you need traffic information for specific IPs or protocols apply a filter based on the corresponding IP/port for each item you want to monitor
- Or: If you do not need long term accounting data and only want to know the current and recent traffic by IP or protocol, you can create just one Packet Sniffer sensor and enable the Toplist feature based on IP or protocol.

A2: Monitoring Total Network traffic with NetFlow

- Configure NetFlow protocol on the router to send NetFlow packets to the computer running PRTG (see corresponding knowledge base article)
- (Purchase and) install Network Connector License (also works with 30 day trial license)
- Configure a NetFlow collector in PRTG
- Create a new NetFlow sensor without any filtering to monitor network's total traffic
- Note: If you have several switches/routers you may not see all traffic if you only monitor one device

A3: Monitoring Total Network traffic using a switch with monitoring port

- Using a switch that has a "monitoring port" or "port mirroring" you can then monitor all the traffic in your network. Most unmanaged switches do not have this feature, many managed switches do.
- Port mirroring is used on a network switch to send a copy of all network packets seen on one switch port to a monitoring network connection on another switch port. This is commonly used for network appliances that require monitoring of network traffic, such as an intrusion-detection system. Port mirroring on a Cisco Systems switch is generally referred to as SPAN.
- BTW: You can also use an old fashioned hub. Hubs send all network packets to all ports, but they are of course a lot slower than switches
- Configure the switch(es) to send a copy of all network packets to the IP of the machine running PRTG
- Create a new Packet Sniffer Sensor without any filtering to monitor network's total traffic
- Note: If you have several switches/routers you may not see all traffic if you only monitor one device

B1: Monitoring Network traffic of each PC (or connection) in a network using a switch/router with SNMP support

- Enable SNMP on the switch or router or device and also set the security feature to allow PRTG to access the device
- For a windows PC install generic SNMP software from the Windows CD (see corresponding knowledge base article)
- It is a good idea to note down which PC (or device or leased line, etc.) is connected to which port for later reference
- Start the "Add Sensor" wizard, choose SNMP, enter the IP and the SNMP login data of the router/switch
- In the checkbox list check the ports that you want to monitor and finish the wizard
- Now you will get graphs of traffic for each device that is connected to one of the ports of your device
- It is a good idea to double click each sensor in the sensor list and edit the sensor name with name of the actual connection
- If you have several switches/routers/devices you must repeat this procedure for each device until you have created a sensor for each port

B2: Monitoring Network traffic for each PC (or connection) with NetFlow

- Configure NetFlow protocol on the router to send NetFlow packets to the computer running PRTG (see corresponding knowledge base article)
- (Purchase and) install Network Connector License (also works with trial license)
- Configure a Network collector in PRTG
- Create one new NetFlow sensor for each PC to be monitored and apply a filter based on the IP of each PC you want to monitor
- Or: If you do not need long term accounting data for each PC and only want to know the current traffic by IP, you can create just one NetFlow sensor and enable the Toplist feature.
- Note: If you have several switches/routers you may not see all traffic if you only monitor one device

B3: Monitoring Network traffic for each PC using a switch with monitoring port

- See A3 for monitoring port basics
- Configure the switch(es) to send a copy of all network packets to the IP of the machine running PRTG

- Create one new Packet Sniffer sensor for each PC to be monitored and apply a filter based on the MAC address or IP of each PC you want to monitor
- Or: If you do not need long term accounting data for each PC and only want to know the current and recent traffic by IP, you can create just one Packet Sniffer sensor and enable the Toplist feature based on IP.
- Note: If you have several switches/routers you may not see all traffic if you only monitor one device

C2: Monitoring network traffic by IP address or protocol with NetFlow

- Configure NetFlow protocol on the router to send NetFlow packets to the computer running PRTG (see corresponding knowledge base article)
- (Purchase and) install Netflowk Collector License (also works with trial license)
- Configure a Netflow collector in PRTG
- Create one new NetFlow sensor for each IP or protocol to be monitored and apply a filter based on the IP or protocol for each item you want to monitor
- Or: If you do not need long term accounting data for each PC and only want to know the current and recent traffic by IP or protocol, you can create just one NetFlow sensor and enable the Toplist feature based on IP or protocol.
- Note: If you have several switches/routers you may not see all traffic if you only monitor one device

C3: Monitoring network traffic by IP address or protocol using a switch with monitoring port

- See A3 for monitoring port basics
- Configure the switch(es) to send a copy of all network packets to the IP of the machine running PRTG
- Create one new Packet Sniffer sensor for each IP/protocol to be monitored and apply a filter based on the corresponding IP/port for each item you want to monitor
- Or: If you do not need long term accounting data for each PC and only want to know the current and recent traffic by IP or protocol, you can create just one Packet Sniffer sensor and enable the Toplist feature based on IP or protocol.
- Note: If you have several switches/routers you may not see all traffic if you only monitor one device

D1: Monitoring Network traffic for a PC running PRTG using SNMP

- Install and enable generic SNMP software from the Windows CD (see corresponding knowledge base article)
- Set the security feature to allow PRTG to access the device
- Start the "Add Sensor" wizard, choose SNMP, enter the local PC's IP and the SNMP login data
- In the checkbox list check the ports (which correspond to the network cards in this case) that you want to monitor and finish the wizard
- Now you will get graphs of traffic for each network card

D3: Monitoring Network traffic for a PC running PRTG using Packet Sniffing

- Create one new Packet Sniffer sensor for each network card to be monitored

E3: Monitoring Network traffic for a PC running PRTG using Packet Sniffing

- Create one new Packet Sniffer sensor for each IP/protocol and for each network card to be monitored and apply a filter based on the corresponding IP/port for each item you want to monitor
- Or: If you do not need long term accounting data for each IP or protocol and only want to know the current and recent traffic by IP or protocol, you can create just one Packet Sniffer sensor and enable the Toplist feature based on IP or protocol.

F1: Monitoring total Network traffic of a shared Internet connection or leased line using a switch/router with SNMP support

- Enable SNMP on the switch or router or device and also set the security feature to allow PRTG to access the device
- Find out which port (i.e. port number) the shared connection is attached to
- Start the "Add Sensor" wizard, choose SNMP, enter the IP and the SNMP login data of the router/switch
- In the checkbox list check the box of the port the shared connection is attached to and finish the wizard
- Now you will get a graph of traffic of the shared line

G2: Monitoring network traffic by IP address or protocol of a shared Internet connection or leased line - Monitoring with NetFlow

- See C2, but select filtering to exclude the LAN IPs

G3: Monitoring network traffic by IP address or protocol of a shared Internet connection or leased line - Monitoring with Packet Sniffing

- See C3, but select filtering to exclude the LAN IPs

First Steps with PRTG Traffic Grapher

Please read the following „Basic Concepts“ section in order to get a clear overview of the basic premises required for the proper operation of PRTG Traffic Grapher.

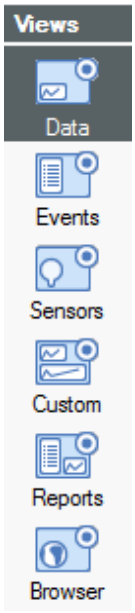
Basic Concepts: Understanding Views, Sensors, Graphs, Charts, Tables, and Tags

To understand the concepts of PRTG Traffic Grapher please be aware of following phrases:

Views

PRTG offers various ways to look at the collected data. We call these “views”. There are six different views. You can switch between the views on the left of the main window:

- **Data:** Shows the collected data of one or more sensors in graphs and tables
- **Events:** Shows a list of events for all sensors or the selected sensors
- **Sensors:** This view is perfect for organizing your continuously growing list of sensors
- **Custom:** In this view you can create your own custom layout of graphs, charts, and tables
- **Reports:** PRTG includes a powerful reporting engine which also includes a billing system
- **Web Browser:** Here you can access the Web interface of PRTG Traffic Grapher

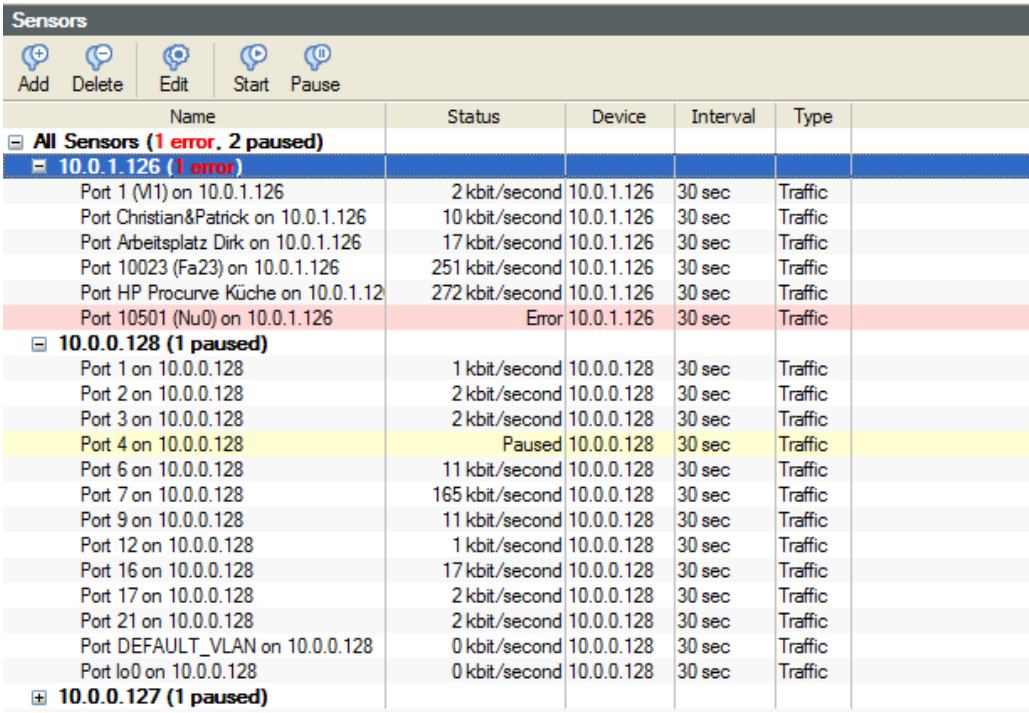


Sensors

Depending on the method of data acquisition one "sensor" can be:

- **For SNMP traffic sensors:** One sensor monitors the in- and out-going traffic of one port of a device (e.g. a port of a switch or a network card of a PC)
- **For other SNMP Sensors:** A sensor monitors one single parameter (e.g. the CPU usage or room temperature)
- **For Packet Sniffing:** One sensor monitors all traffic going through one or more network cards. Several sensors can monitor the same network card using different filter settings (e.g. to monitor only specific IPs or protocols)
- **For NetFlow monitoring:** One sensor monitors all NetFlow data packets arriving at one NetFlow Collector. Usually one Network Collector is installed per switch. Several sensors can monitor the same NetFlow Collector using different filter settings (e.g. to monitor only specific IPs or protocols)
- **For Latency monitoring:** One sensor records the PING times for one remote IP address

In the main window the list of all sensors can be seen. Each sensor is shown with its current reading, device, interval and type. The colors red and yellow show error and paused sensor states.

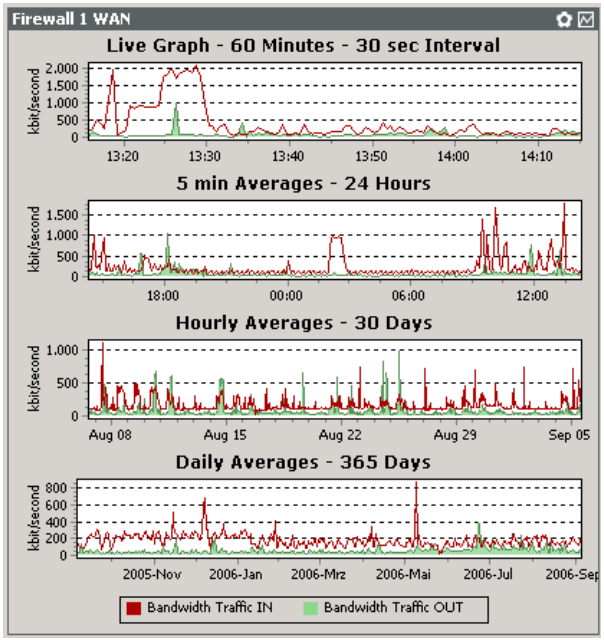

Sensors
Add
Delete
Edit
Start
Pause
Name
Status
Device
Interval
Type
All Sensors (1 error, 2 paused)
10.0.1.126 (1 error)
Port 1 (M1) on 10.0.1.126 2 kbit/second 10.0.1.126 30 sec Traffic
Port Christian&Patrick on 10.0.1.126 10 kbit/second 10.0.1.126 30 sec Traffic
Port Arbeitsplatz Dirk on 10.0.1.126 17 kbit/second 10.0.1.126 30 sec Traffic
Port 10023 (Fa23) on 10.0.1.126 251 kbit/second 10.0.1.126 30 sec Traffic
Port HP Procurve Küche on 10.0.1.12 272 kbit/second 10.0.1.126 30 sec Traffic
Port 10501 (Nu0) on 10.0.1.126 Error 10.0.1.126 30 sec Traffic
10.0.0.128 (1 paused)
Port 1 on 10.0.0.128 1 kbit/second 10.0.0.128 30 sec Traffic
Port 2 on 10.0.0.128 2 kbit/second 10.0.0.128 30 sec Traffic
Port 3 on 10.0.0.128 2 kbit/second 10.0.0.128 30 sec Traffic
Port 4 on 10.0.0.128 Paused 10.0.0.128 30 sec Traffic
Port 6 on 10.0.0.128 11 kbit/second 10.0.0.128 30 sec Traffic
Port 7 on 10.0.0.128 165 kbit/second 10.0.0.128 30 sec Traffic
Port 9 on 10.0.0.128 11 kbit/second 10.0.0.128 30 sec Traffic
Port 12 on 10.0.0.128 1 kbit/second 10.0.0.128 30 sec Traffic
Port 16 on 10.0.0.128 17 kbit/second 10.0.0.128 30 sec Traffic
Port 17 on 10.0.0.128 2 kbit/second 10.0.0.128 30 sec Traffic
Port 21 on 10.0.0.128 2 kbit/second 10.0.0.128 30 sec Traffic
Port DEFAULT_VLAN on 10.0.0.128 0 kbit/second 10.0.0.128 30 sec Traffic
Port lo0 on 10.0.0.128 0 kbit/second 10.0.0.128 30 sec Traffic
10.0.0.127 (1 paused)

Sensors are organized in groups and you can rearrange the order of the sensors using drag&drop.

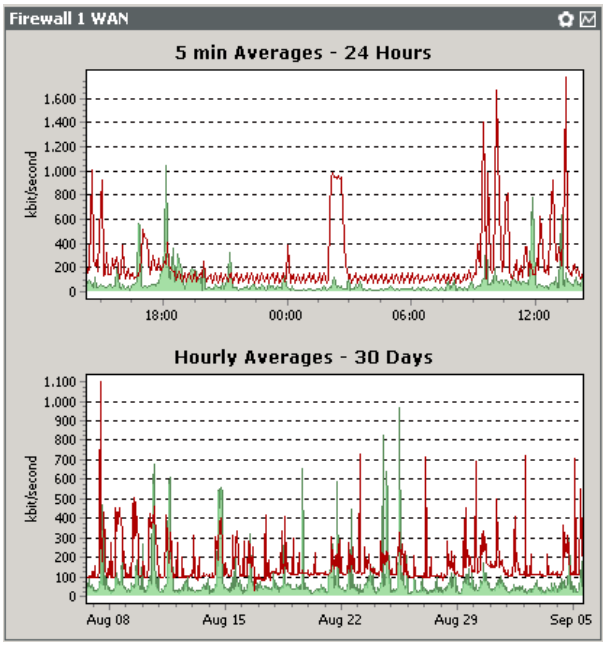
Graphs and Charts

One “Graph”, graphically showing the monitoring results of one or more sensors, contains up to four “Charts”, selectable by the user.

E.g. this graph shows four charts:

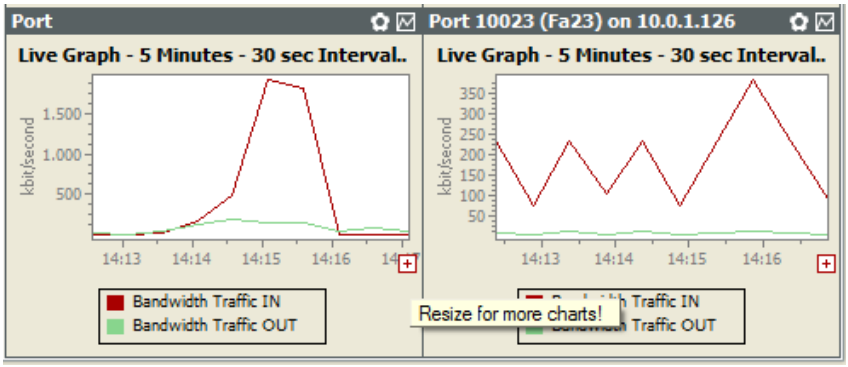


A graph can also be set to only show two charts, or even just one:



PRTG automatically hides titles, footers, legends and even complete charts from a graph if the available screen space does not allow to show the graphs completely.

In this case you will see a small red "PLUS" logo at the bottom right:



Tables

Besides graphs PRTG Traffic Grapher also offers various "Tables". These tables show the monitoring results in detailed numerical grids.

Table: Firewall 1 WAN (365 Days, Daily Averages)

	Firewall 1 WAN						
	Bandwidth Traffic IN		Bandwidth Traffic OUT		Sum		Coverage
	kbyte	kbit/second	kbyte	kbit/second	kbyte	kbit/second	%
05.09.2006	1.590.935,672	255,544	363.350,722	58,432	1.954.286,394	313,976	59
04.09.2006	1.825.517,925	174,458	698.151,553	66,743	2.523.669,478	241,201	99
03.09.2006	1.225.069,249	116,173	353.269,010	33,500	1.578.338,259	149,673	100
02.09.2006	1.519.496,342	144,094	377.989,941	35,845	1.897.486,283	179,939	100
01.09.2006	1.537.227,927	145,774	377.717,331	35,819	1.914.945,258	181,593	100
31.08.2006	1.861.678,975	176,541	553.071,148	52,447	2.414.750,123	228,988	100
30.08.2006	2.259.422,099	214,413	658.636,034	62,459	2.918.058,133	276,872	100
29.08.2006	1.776.060,626	168,422	607.746,873	57,632	2.383.807,499	226,054	100
28.08.2006	1.491.731,334	141,461	592.905,593	56,225	2.084.636,927	197,686	100
27.08.2006	1.437.853,377	136,351	395.779,397	37,531	1.833.632,774	173,882	100
26.08.2006	1.124.183,282	106,606	367.286,397	34,830	1.491.469,680	141,436	100
25.08.2006	1.737.681,511	164,783	1.133.839,894	107,521	2.871.521,404	272,304	100
24.08.2006	1.679.935,509	159,418	1.528.126,099	144,911	3.208.061,607	304,329	100
23.08.2006	1.789.462,974	169,696	626.317,743	59,394	2.415.780,717	229,090	100
22.08.2006	1.546.241,351	146,629	721.698,024	68,438	2.267.939,375	215,067	100
21.08.2006	1.698.488,488	161,067	1.175.477,087	111,471	2.873.965,575	272,538	100
20.08.2006	1.265.230,707	119,982	328.425,205	31,145	1.593.655,912	151,127	100
19.08.2006	1.366.728,544	129,606	817.925,854	77,564	2.184.654,398	207,170	100

For Packet Sniffer and NetFlow Sensors you will also see so-called Toplists with lists of the Top Talkers, Top Protocols and Top Connections. For each sensor you can also configure additional customized toplists.

Top Protocols: PEPE

05.09.2006 14:15:00 - 05.09.2006 14:30:00 (Note: Doubleclick the list to access previous intervalls!)

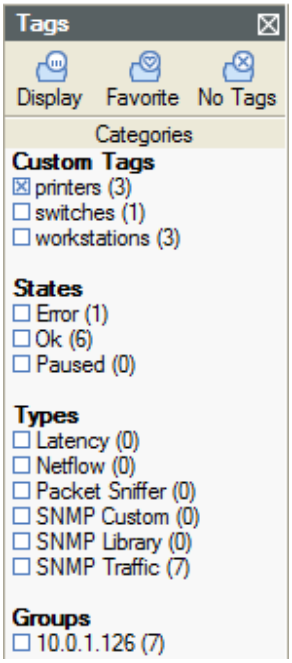
	Channel	Volume	Trend (97%)
1	HTTP	790 kbytes	
2	Other	110 kbytes	
3	SNMP	45887 bytes	
4	NETBIOS	5619 bytes	
5	DNS	2844 bytes	
6	FTP	572 bytes	
7	RDP	206 bytes	
8	ICMP	148 bytes	

Tags

A tag is a keyword or descriptive term associated with a sensor as means of classification. Tags will especially help you if you have a large number of sensors.

After sorting sensors into groups the method of tagging is a second way to categorize your sensors. For example you can group the sensors in your sensorlist by device (“Switch 1”, “Switch 2” and “Switch 3”).

Now you can associate the tag “printers” to all switch ports that are connected to printers. Now you can click on “printers” in the taglist and PRTG will only show the sensors which are associated with the “printers” tag.



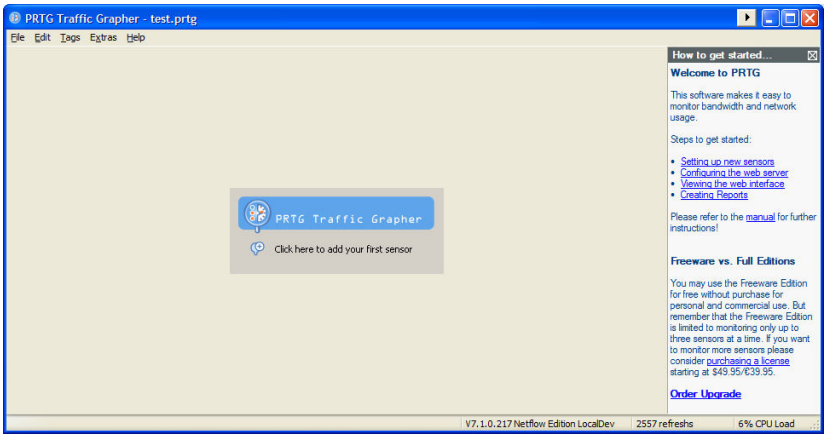
Tags are created by the user (you can enter any number of tags for one or more sensors) and automatically created by PRTG (e.g. the tag “OK” for a sensor that works fine or “Error” for a sensor that shows an error),

Tagging allows for multiple "browseable paths" through the items which can quickly and easily be altered with minimal effort and planning.

In the main window you can click on the **Display** button above the taglist to change the sort order of the tags. Click on **Favorite** to save the current tag combination into a favorite. Click on **No Tags** to disable the filtering and to see all sensors again.

Starting PRTG for the first time

After installation, when starting PRTG Traffic Grapher for the first time, a window will appear showing the following information:


PRTG Traffic Grapher - test.prtg
File Edit Tags Extras Help
How to get started...
Welcome to PRTG
This software makes it easy to monitor bandwidth and network usage.
Steps to get started:
Setting up new sensors
Configuring the web server
Viewing the web interface
Creating Reports
Please refer to the manual for further instructions!
Freeware vs. Full Editions
You may use the Freeware Edition for free without purchase for personal and commercial use. But remember that the Freeware Edition is limited to monitoring only up to three sensors at a time. If you want to monitor more sensors please consider purchasing a license starting at $49.95/€39.95.
Order Upgrade
PRTG Traffic Grapher
Click here to add your first sensor
V7.1.0.217 Netflow Edition LocalDev
2557 refreshs
6% CPU Load

Clicking on the button in the middle of the page will launch the **Add Sensor Wizard**. Using this wizard, you can set up your first sensor(s) for monitoring.

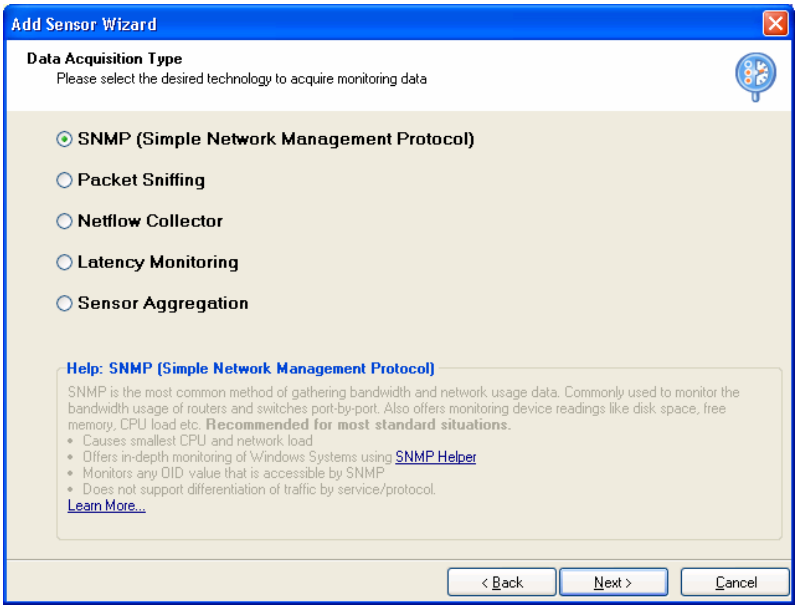
Adding New Sensors using the Add Sensor Wizard

Adding new sensors in PRTG Traffic Grapher is easy. Merely click on **Click here to add you first sensor**: This will show the **Add Sensor Wizard**:

Add Sensor Wizard
Welcome to the Add Sensor Wizard
This wizard will guide you step-by-step through the setup of new sensors for monitoring with PRTG Traffic Grapher.
Creating new sensors involves three main steps:
1. Selecting the data acquisition technology (SNMP, packet sniffing or NetFlow)
2. Selecting the device/server and scanning it for available sensors
3. Selecting the new sensors and choosing a group as well as an interval
Note: If you want PRTG Traffic Grapher to scan your network automatically for SNMP enabled devices please use the Automatic Network Discovery to create SNMP based sensors.
Please click "Next" to continue!
PAESSLER
< Back
Next >
Cancel

The Add Sensor Wizard will guide you through the setup of new sensors for monitoring with PRTG Traffic Grapher.

After having read the information on the title screen, press **Next** to continue on to the Data Acquisition Type Selection screen.


Add Sensor Wizard
Data Acquisition Type
Please select the desired technology to acquire monitoring data
SNMP (Simple Network Management Protocol)
Packet Sniffing
Netflow Collector
Latency Monitoring
Sensor Aggregation
Help: SNMP (Simple Network Management Protocol)
SNMP is the most common method of gathering bandwidth and network usage data. Commonly used to monitor the bandwidth usage of routers and switches port-by-port. Also offers monitoring device readings like disk space, free memory, CPU load etc. Recommended for most standard situations.
Causes smallest CPU and network load
Offers in-depth monitoring of Windows Systems using SNMP Helper
Monitors any OID value that is accessible by SNMP
Does not support differentiation of traffic by service/protocol.
Learn More...
< Back
Next >
Cancel

Here you can select which type of sensor you would like to monitor from the choices provided:

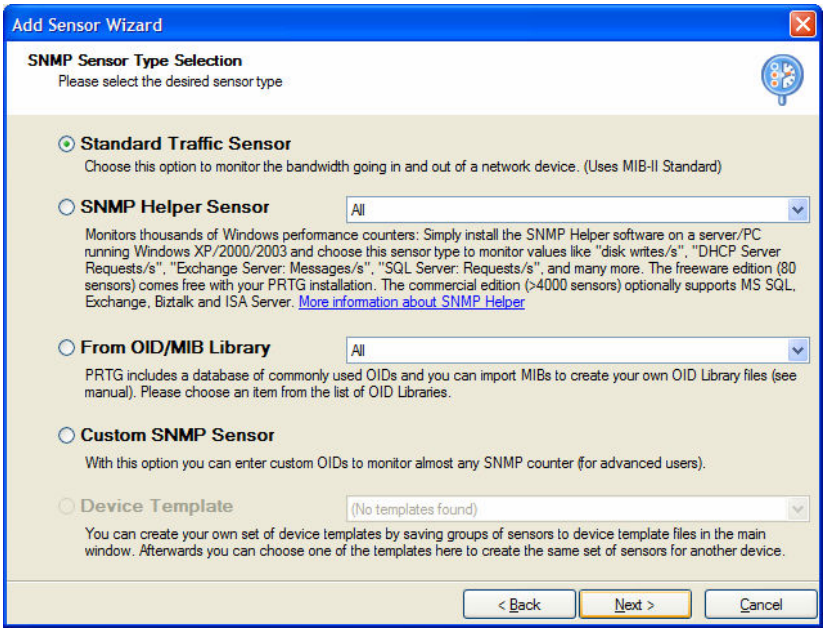
- SNMP

- Packet Sniffing
- NetFlow Collector
- Latency Monitoring
- Sensor Aggregation

All types are explained in-depth later in this manual.

For this sample, we will create an SNMP sensor since this is the most common option.

Please select **SNMP** and click **Next**.

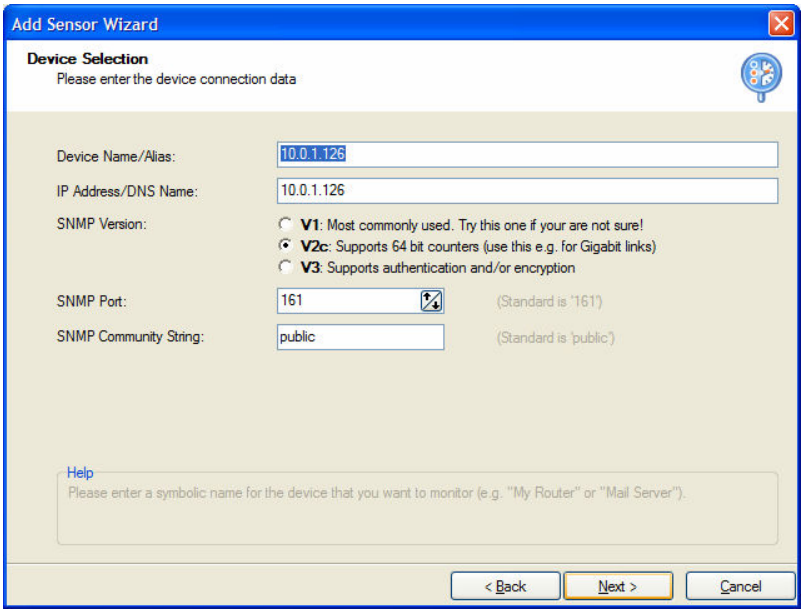

Add Sensor Wizard
SNMP Sensor Type Selection
Please select the desired sensor type
Standard Traffic Sensor
Choose this option to monitor the bandwidth going in and out of a network device. (Uses MIB-II Standard)
SNMP Helper Sensor
All
Monitors thousands of Windows performance counters: Simply install the SNMP Helper software on a server/PC running Windows XP/2000/2003 and choose this sensor type to monitor values like "disk writes/s", "DHCP Server Requests/s", "Exchange Server: Messages/s", "SQL Server: Requests/s", and many more. The freeware edition (80 sensors) comes free with your PRTG installation. The commercial edition (>4000 sensors) optionally supports MS SQL, Exchange, Biztalk and ISA Server. More information about SNMP Helper
From OID/MIB Library
All
PRTG includes a database of commonly used OIDs and you can import MIBs to create your own OID Library files (see manual). Please choose an item from the list of OID Libraries.
Custom SNMP Sensor
With this option you can enter custom OIDs to monitor almost any SNMP counter (for advanced users).
Device Template
(No templates found)
You can create your own set of device templates by saving groups of sensors to device template files in the main window. Afterwards you can choose one of the templates here to create the same set of sensors for another device.
< Back
Next >
Cancel

Here, you can select the type of SNMP sensor you would like to monitor. The options are:

- **Standard Traffic Sensor**
- **SNMP Helper Sensor**
- **From OID/MIB Library**
- **Custom SNMP Sensor**
- **Device Template**

For this tutorial we will create a **Standard Traffic Sensor** (you need to have a compatible device in your network). Select the appropriate type of sensor from the list and click **Next** to continue.

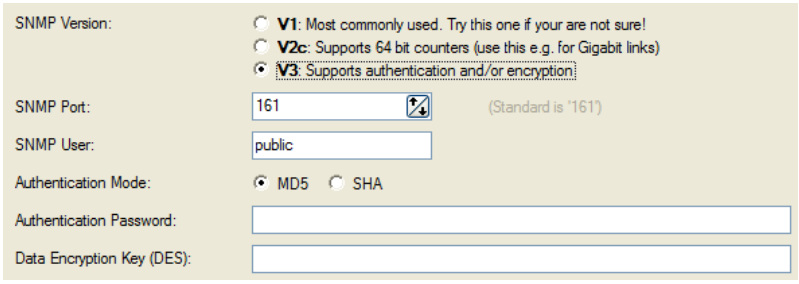
This will launch the **Device Selection** screen.


Add Sensor Wizard
Device Selection
Please enter the device connection data
Device Name/Alias:
10.0.1.126
IP Address/DNS Name:
10.0.1.126
SNMP Version:
V1: Most commonly used. Try this one if your are not sure!
V2c: Supports 64 bit counters (use this e.g. for Gigabit links)
V3: Supports authentication and/or encryption
SNMP Port:
161
(Standard is '161')
SNMP Community String:
public
(Standard is 'public')
Help
Please enter a symbolic name for the device that you want to monitor (e.g. "My Router" or "Mail Server").
< Back
Next >
Cancel

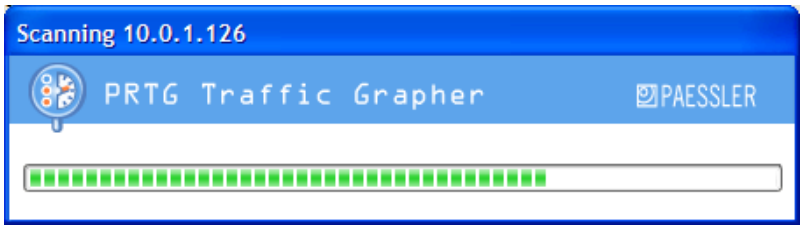
Here, you will need to enter a **Device Name/Alias** for the sensor you would like to set up. Next, you will need to enter the **IP Address/DNS Name** of the device you would like to monitor.

If you want to use SNMP Version 1 or 2c you may also need to update the **SNMP community string**, as well as the **SNMP port**. Usually it should be fine to keep the defaults ("public" for the SNMP Community String and "161" for the SNMP port). Contact your network admin if you are not sure.

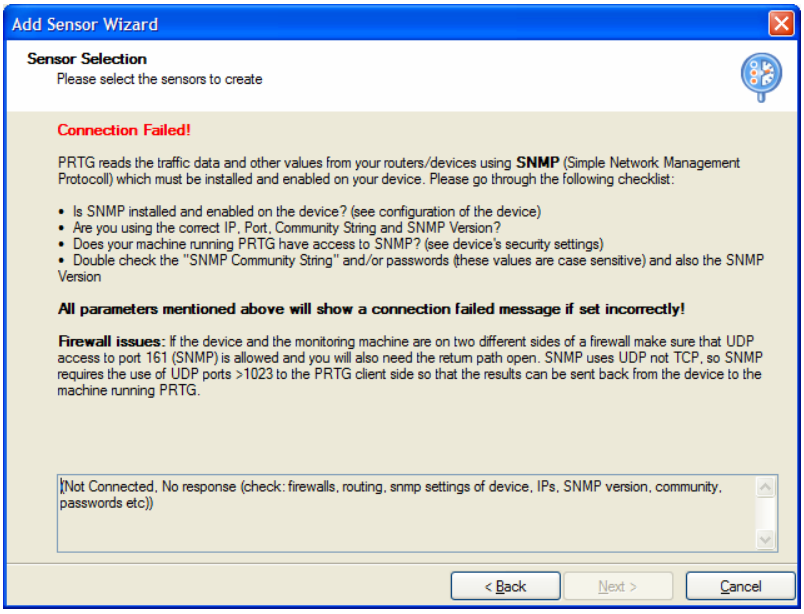
If you are using SNMP V3 you also have to enter the **SNMP User**, **Authentication Mode** and **Password,** as well as the optional **Data Encryption** key.



Click **Next** to continue. Now PRTG Traffic Grapher tries to contact the device for the first time.



If the connection fails you will get an error message. In this case, please follow the instructions on the screen!

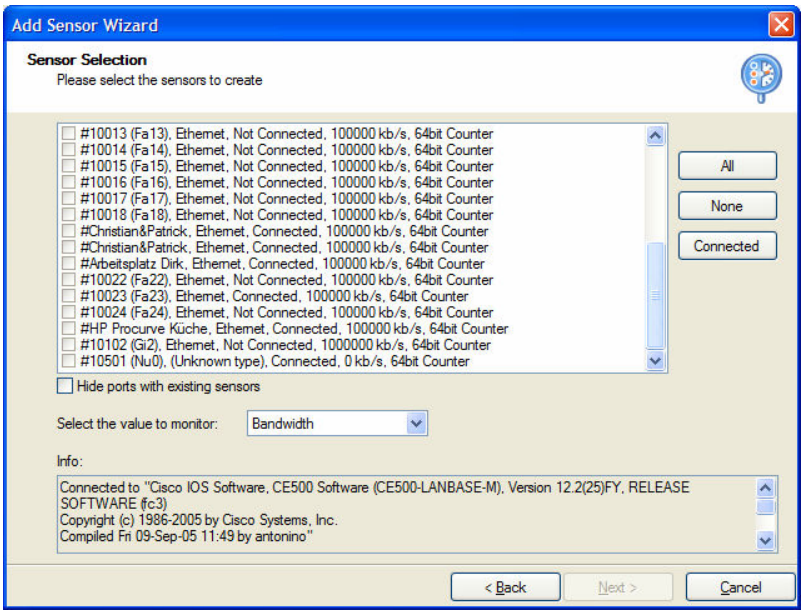

Add Sensor Wizard
Sensor Selection
Please select the sensors to create
Connection Failed!
PRTG reads the traffic data and other values from your routers/devices using SNMP (Simple Network Management Protocol) which must be installed and enabled on your device. Please go through the following checklist:
• Is SNMP installed and enabled on the device? (see configuration of the device)
• Are you using the correct IP, Port, Community String and SNMP Version?
• Does your machine running PRTG have access to SNMP? (see device's security settings)
• Double check the "SNMP Community String" and/or passwords (these values are case sensitive) and also the SNMP Version
All parameters mentioned above will show a connection failed message if set incorrectly!
Firewall issues: If the device and the monitoring machine are on two different sides of a firewall make sure that UDP access to port 161 (SNMP) is allowed and you will also need the return path open. SNMP uses UDP not TCP, so SNMP requires the use of UDP ports >1023 to the PRTG client side so that the results can be sent back from the device to the machine running PRTG.
[Not Connected, No response (check: firewalls, routing, snmp settings of device, IPs, SNMP version, community, passwords etc)]
< Back
Next >
Cancel

The most common reason for connection problems are incorrect IP addresses, SNMP Port or community string – they all show a **connection failed** error. The second most common problem are connection issues due to firewalls that block the UDP traffic.

It is important to know that if you select an SNMP version which is not supported by the server or device that you want to monitor you will also receive this error message!

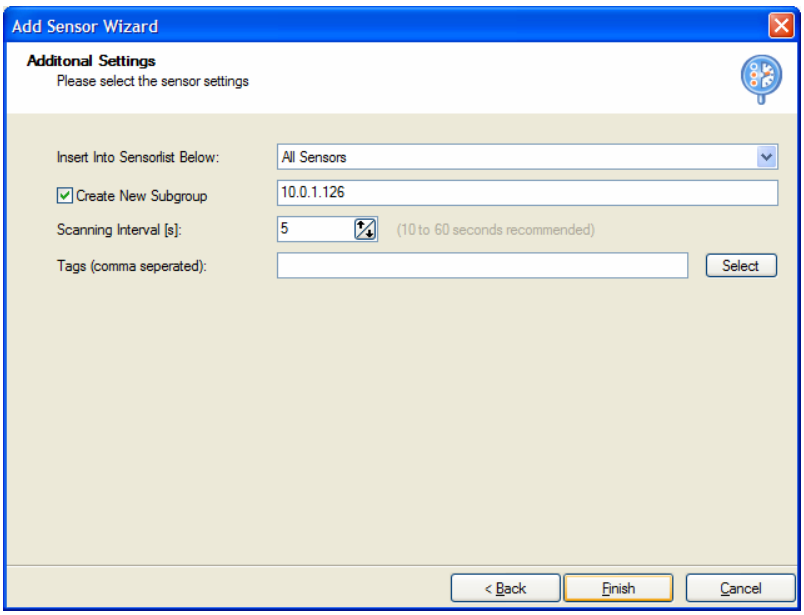
Unfortunately most of the time these error messages are not explicitly telling you about the incorrect SNMP version (they say only something like "cannot connect" or similar). The same situation exists if community string, usernames and passwords are incorrect.

If the connection works you will be shown the **Port Selection**:


Add Sensor Wizard
Sensor Selection
Please select the sensors to create
#10013 (Fa13), Ethernet, Not Connected, 100000 kb/s, 64bit Counter
#10014 (Fa14), Ethernet, Not Connected, 100000 kb/s, 64bit Counter
#10015 (Fa15), Ethernet, Not Connected, 100000 kb/s, 64bit Counter
#10016 (Fa16), Ethernet, Not Connected, 100000 kb/s, 64bit Counter
#10017 (Fa17), Ethernet, Not Connected, 100000 kb/s, 64bit Counter
#10018 (Fa18), Ethernet, Not Connected, 100000 kb/s, 64bit Counter
#Christian&Patrick, Ethernet, Connected, 100000 kb/s, 64bit Counter
#Christian&Patrick, Ethernet, Connected, 100000 kb/s, 64bit Counter
#Arbeitsplatz Dirk, Ethernet, Connected, 100000 kb/s, 64bit Counter
#10022 (Fa22), Ethernet, Not Connected, 100000 kb/s, 64bit Counter
#10023 (Fa23), Ethernet, Connected, 100000 kb/s, 64bit Counter
#10024 (Fa24), Ethernet, Not Connected, 100000 kb/s, 64bit Counter
#HP Procurve Küche, Ethernet, Connected, 100000 kb/s, 64bit Counter
#10102 (Gi2), Ethernet, Not Connected, 1000000 kb/s, 64bit Counter
#10501 (Nu0), (Unknown type), Connected, 0 kb/s, 64bit Counter
All
None
Connected
Hide ports with existing sensors
Select the value to monitor:
Bandwidth
Info:
Connected to "Cisco IOS Software, CE500 Software (CE500-LANBASE-M), Version 12.2(25)FY, RELEASE SOFTWARE (fc3)
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Fri 09-Sep-05 11:49 by antonino"
< Back
Next >
Cancel

The screen sprovides a list of the ports that PRTG has found and that are available for monitoring. Using the mouse check one or more entries you would like PRTG Traffic Grapher to monitor. You can also use the shortcut buttons **All**, **None** and **Connected** to select the ports. Clicking the **Hide ports with existing sensors** checkbox will remove all ports that have already a sensor from the list to prvent dublicate monitoring.

At the bottom of the windows you can select whether you want to monitor the **Bandwidth** (most common choice), number of **Unicast-Packets**, **Non-Unicast-Packets,** or **Errors**. Then click **Next** in order to set up the **Additional Settings**.



Choose a group from the sensor list that you want to add the new sensor(s) to. Optionally you can **Create a New Subgroup**.

Choose a group name that will help you to keep your sensors organized (e.g. “Firewall” or “LAN”). Also select the desired **scanning interval** in seconds. In most cases 30 seconds should be fine.

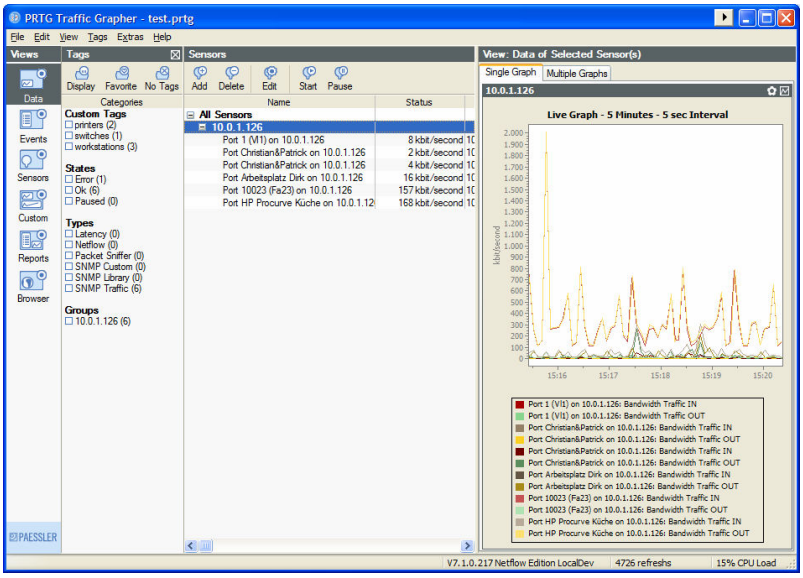
Note: Small intervals create higher network load but will give you a more “current view” of the measured data. Longer intervals will cause smaller network load but the measured data will be more “averaged”.

Finally you can add tags for the new sensors which will help you to categorize your sensors later. A tag can be one or more words, e.g. switch, printer, 1st floor, 2nd floor, remote office, data center 1, data center 2, etc. Use commas to separate tags.

Once you have selected your preferences, click on **Finish** and PRTG Traffic Grapher will begin monitoring your newly defined sensor(s) in a few seconds.

A First Look at The Main Window

As soon as you have created one or more sensors you will see this layout of the main Window:



From left to right the main window consists of four areas:

- Views
- Tags
- Sensors
- Data of selected Sensors

On the left you can switch between PRTG's six different views of the data. In the sensor list you can choose one sensor, several sensors (hold down CTRL and/or shift while selecting more than one entry), or groups of sensors.

Double click a sensor to edit the sensor. Also various context sensitive pop-up menus can be brought up throughout the interface by clicking the right mouse button.

See the next section for more information on the usage of PRTG Traffic Grapher.

Using the Windows GUI

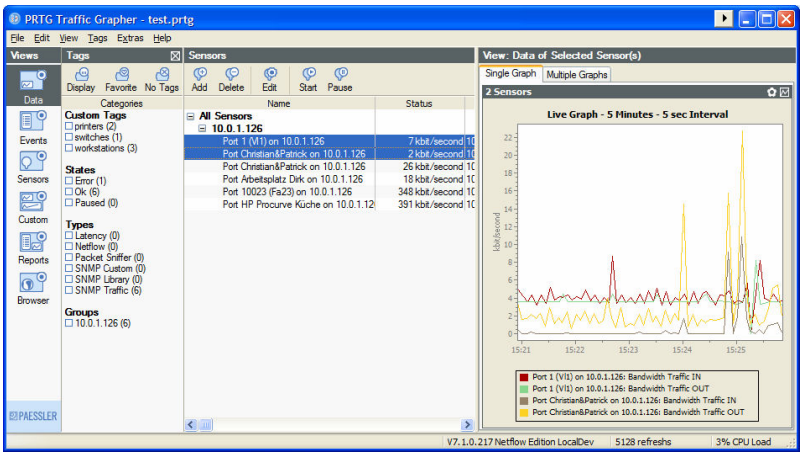
Navigating Views, Sensors, Graphs, and Tags

This section will tell you how to use the views, sensors, graphs, tables, and tags. If you are not yet familiar with these terms please have a look at the Basic Concepts:

Understanding Views, Sensors, Graphs, Charts, Tables, and Tags section for explanations.

PRTG's Main Window

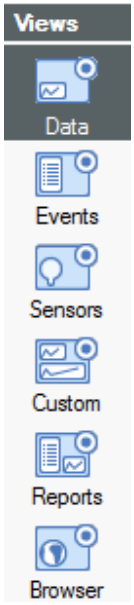
The main window of PRTG Traffic Grapher consists of four main areas:



On the left you can see the area used to select the current view, followed by the taglist. The list of sensors can be found in the middle and on the right you can see the area for the monitoring data.

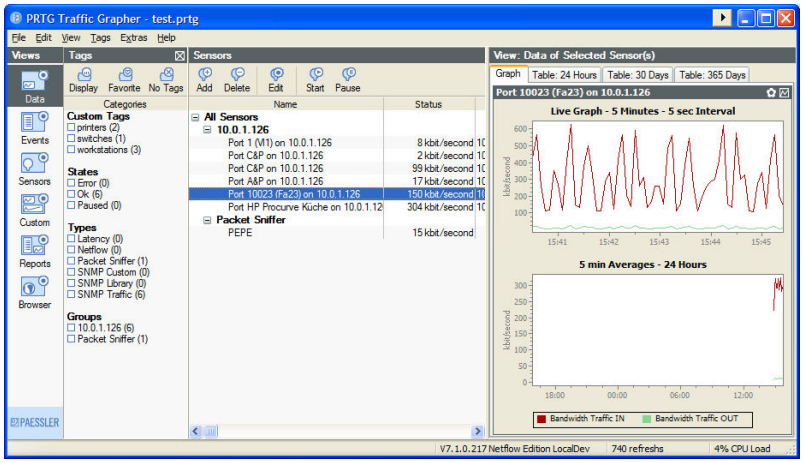
Available Views

There are six different views that you can select by clicking the corresponding icons on the left:



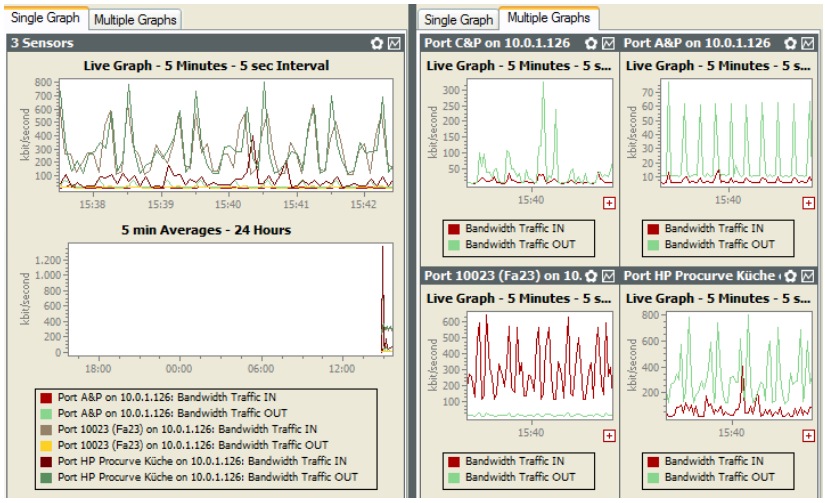
Data View

This view shows the collected data of one or mores sensors in one graph.

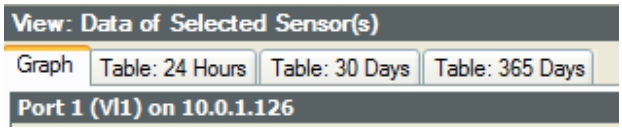


To visualize the data of more than one sensor you can select several sensors from the list of sensors. Simply use CTRL while clicking an item to select disjointed items from the list, or use SHIFT while clicking an icon to select several sensors. Or, select a group.

If a group or more than one sensor are selected you can switch between Single Graph (the data of all sensors is shown in one chart, shown on the left) and Multiple Graphs (one graph for the data of each sensor, on the right):


Single Graph
Multiple Graphs
3 Sensors
Live Graph - 5 Minutes - 5 sec Interval
5 min Averages - 24 Hours
Port A&P on 10.0.1.126: Bandwidth Traffic IN
Port A&P on 10.0.1.126: Bandwidth Traffic OUT
Port 10023 (Fa23) on 10.0.1.126: Bandwidth Traffic IN
Port 10023 (Fa23) on 10.0.1.126: Bandwidth Traffic OUT
Port HP Procurve Küche on 10.0.1.126: Bandwidth Traffic IN
Port HP Procurve Küche on 10.0.1.126: Bandwidth Traffic OUT
Port C&P on 10.0.1.126
Port A&P on 10.0.1.126
Port 10023 (Fa23) on 10.
Port HP Procurve Küche
Bandwidth Traffic IN
Bandwidth Traffic OUT

If only one sensor is selected you can choose between graphs and three data tables on the right:



These data tables show the data for the last 24 or 48 hours, last 30 days, or last 365 days (these periods can be changed in the options) :

View: Data of Selected Sensor(s)

Graph | Table: 24 Hours | Table: 30 Days | Table: 365 Days

Table: Port 1 (VI1) on 10.0.1.126 (24 Hours, 5 min Averages)

	Port 1 (VI1) on 10.0.1.126						
	Bandwidth Traffic IN		Bandwidth Traffic OUT		Sum		Coverage
	kbyte	kbit/second	kbyte	kbit/second	kbyte	kbit/second	%
05.09.2006 15:30 - 15:35							
05.09.2006 15:25 - 15:30	147,198	4,025	132,375	3,619	279,573	7,644	100
05.09.2006 15:20 - 15:25	149,278	4,082	132,550	3,624	281,828	7,706	100
05.09.2006 15:15 - 15:20	159,926	4,372	143,359	3,919	303,285	8,292	100
05.09.2006 15:10 - 15:15	158,764	4,341	143,404	3,921	302,168	8,261	100
05.09.2006 15:05 - 15:10	156,252	4,272	142,873	3,906	299,125	8,178	100
05.09.2006 15:00 - 15:05	158,960	4,346	142,132	3,885	301,092	8,231	100
05.09.2006 14:55 - 15:00	155,683	4,255	141,266	3,862	296,948	8,117	100
05.09.2006 14:50 - 14:55	15,225	4,664	13,945	4,277	29,170	8,941	9

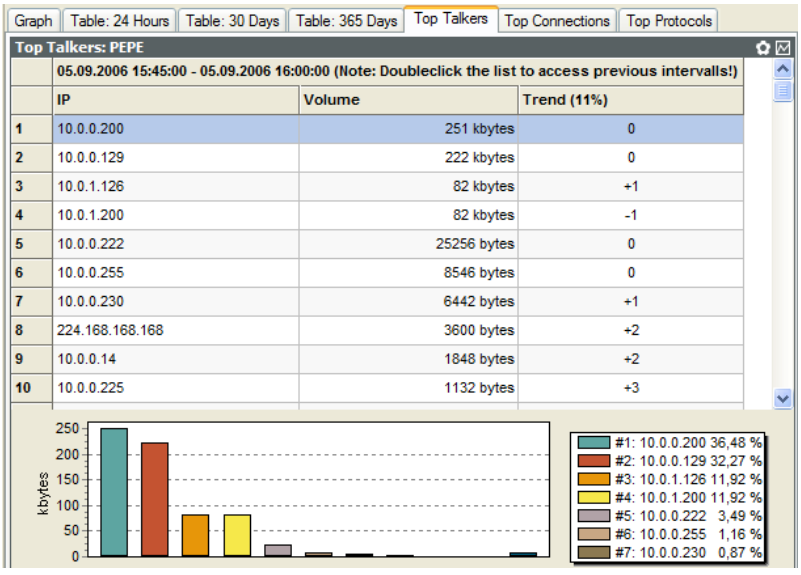
Please note the special column “coverage”: This value tells you if the monitoring was actually working all the time and has covered the complete time period.

E.g. if PRTG is shut down for 15 minutes of an hour you will see a value of 75% of coverage for the remaining 45 minutes that were covered by monitoring.

If you need reliable and full data from your monitoring this value should always be 100% or close to 100%.

If the coverage is below 100% but PRTG was running all the time then there is a technical problem with the sensor. PRTG was not able to get all the data it needs to completely calculate the traffic over time. Most common reasons are network problems (e.g. packet loss, connectivity issues) and device problems (e.g. some devices limit the number of SNMP request per minute, so if they are scanned too frequently a number of requests remain unanswered).

For Packet Sniffer and NetFlow Sensors you will also see tabs for the so-called Toplists (e.g. with lists of the Top Talkers, Top Protocols and Top Connections). For each sensor you can also configure additional customized toplists.



Toplists can be computed based on source or destination IP and Port as well as other parameters.

In the lists you will see a number of columns for the selected values (e.g. source IP). PRTG tries to resolve the IP addresses into DNS names if possible. IP addresses shown in brackets could not be resolved by reverse DNS.

The **Trend** column shows a value that is calculated by subtracting the current position in the list with the position of the previous toplist interval. A value of zero (0) means that an entry is at the same position in the list as in the previous interval, +5 means that the entry has climbed 5 positions. PRTG shows big changes in the list position with a background in various shades of a red to make it easy to see sudden changes.

The pie or bar chart (you can choose the type in the **View|Colors & Layout** dialog) always shows the data volume of the top 10 entries.

Events View

PRTG records an event everytime a sensor shows an error and becomes available again or a custom notification is triggered. You can review the list of these events in the Events view:

View: Events

Time	Kind	Sensor	Message
05.09.2006 15:56:40	Error	Port A&P on 10.0.1.126	Error Notification: UP
05.09.2006 15:56:20	Error	Port A&P on 10.0.1.126	Error Notification: DOWN, Unknown user name
05.09.2006 15:56:15	Error	Port A&P on 10.0.1.126	Error Notification: UP
05.09.2006 15:55:46	Error	Port A&P on 10.0.1.126	Error Notification: DOWN, Unknown user name
05.09.2006 15:50:48	Error	PEPE	Error Notification: DOWN,
05.09.2006 14:54:34	Error	<deleted>	Error Notification: DOWN, No such instance
05.09.2006 13:50:08	Error	<deleted>	Error Notification: DOWN, No such instance
24.08.2006 17:03:36	Error	<deleted>	Error Notification: DOWN, No such instance

In order to see all events of all sensors go to the **Events** view and select the topmost node **All Sensors** from the sensorlist.

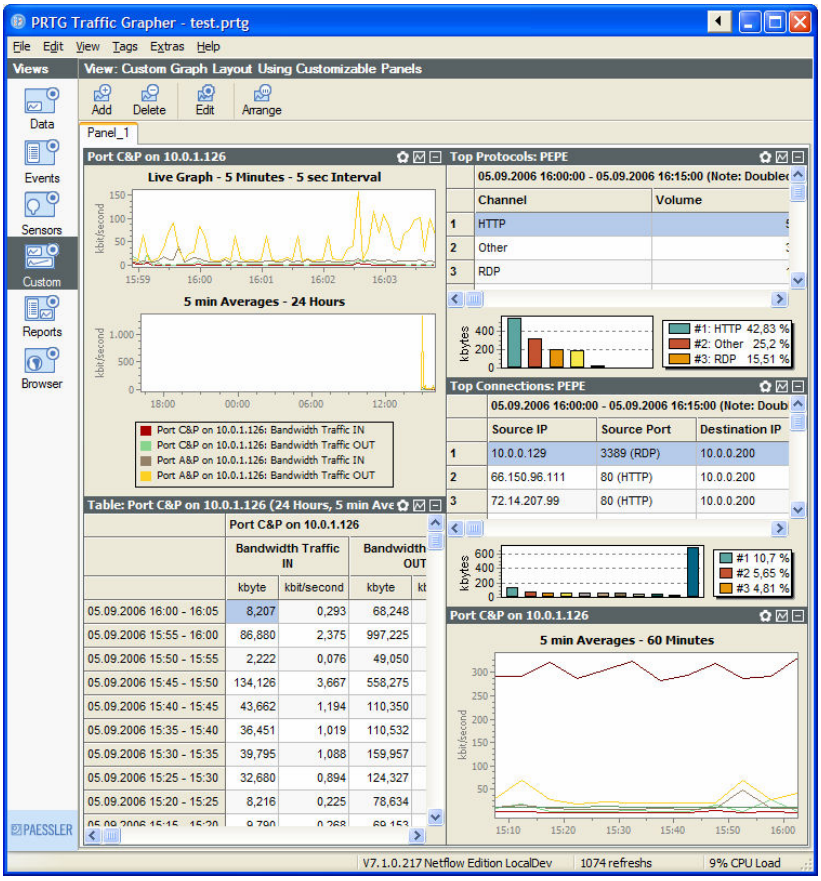
By selecting a group or a single sensor you can filter out the events for the selected sensors.

Sensors View

In this view you can see the list of sensors only without any graphs or data tables (which could slow down the interface for large installations). This view is best suited to administer your sensors, add new ones, or arrange them.

Custom View

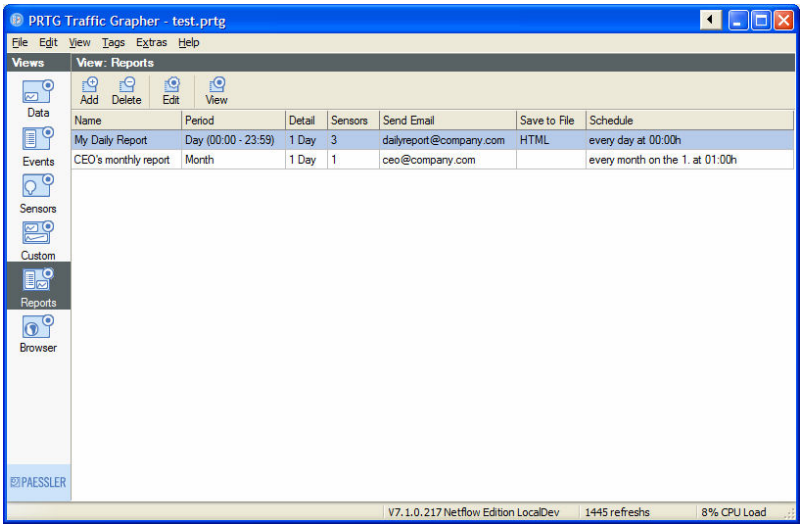
While in Data view the graphs are arranged automatically by PRTG. The Custom view enables you to set up a custom layout of panels, graphs, and tables. You can choose you own layout, mix data tables and graphs from various sensors into a dashboard of information.


PRTG Traffic Grapher - test.prtg
File Edit View Tags Extras Help
Views
View: Custom Graph Layout Using Customizable Panels
Add Delete Edit Arrange
Data
Events
Sensors
Custom
Reports
Browser
Panel_1
Port C&P on 10.0.1.126
Live Graph - 5 Minutes - 5 sec Interval
5 min Averages - 24 Hours
Port C&P on 10.0.1.126: Bandwidth Traffic IN
Port C&P on 10.0.1.126: Bandwidth Traffic OUT
Port A&P on 10.0.1.126: Bandwidth Traffic IN
Port A&P on 10.0.1.126: Bandwidth Traffic OUT
Top Protocols: PEPE
Channel
Volume
1 HTTP
2 Other
3 RDP
#1: HTTP 42,83 %
#2: Other 25,2 %
#3: RDP 15,51 %
Top Connections: PEPE
Source IP
Source Port
Destination IP
1 10.0.0.129 3389 (RDP) 10.0.0.200
2 66.150.96.111 80 (HTTP) 10.0.0.200
3 72.14.207.99 80 (HTTP) 10.0.0.200
#1 10,7 %
#2 5,65 %
#3 4,81 %
Table: Port C&P on 10.0.1.126 (24 Hours, 5 min Ave
Port C&P on 10.0.1.126
Bandwidth Traffic IN
Bandwidth OUT
kbyte
kbit/second
05.09.2006 16:00 - 16:05 8,207 0,293 68,248
05.09.2006 15:55 - 16:00 86,880 2,375 997,225
05.09.2006 15:50 - 15:55 2,222 0,076 49,050
05.09.2006 15:45 - 15:50 134,126 3,667 558,275
05.09.2006 15:40 - 15:45 43,662 1,194 110,350
05.09.2006 15:35 - 15:40 36,451 1,019 110,532
05.09.2006 15:30 - 15:35 39,795 1,088 159,957
05.09.2006 15:25 - 15:30 32,680 0,894 124,327
05.09.2006 15:20 - 15:25 8,216 0,225 78,634
Port C&P on 10.0.1.126
5 min Averages - 60 Minutes
PAESSLER
V7.1.0.217 Netflow Edition LocalDev
1074 refreshs
9% CPU Load

Please see the Working with Custom Graphs section for details.

Reports View

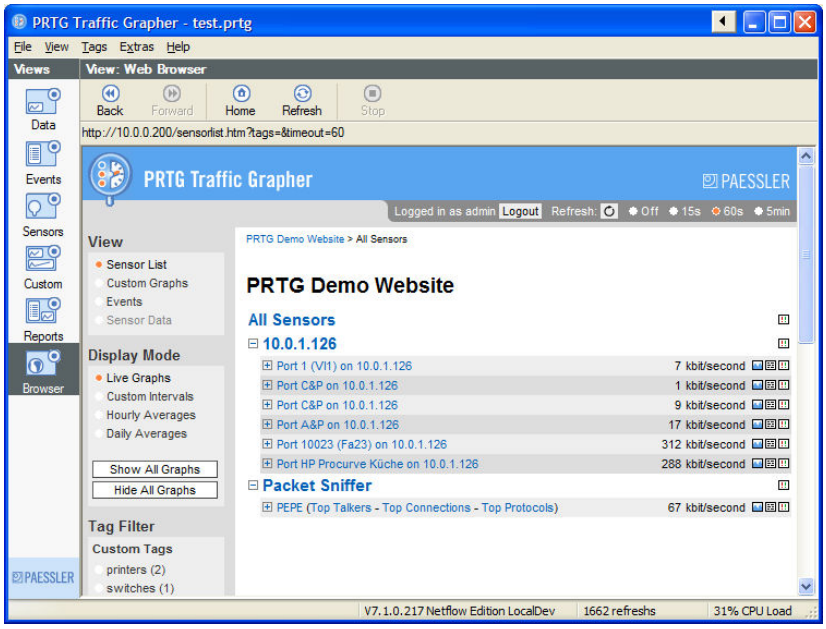
You can define any number of reports that are based on the collected data. These reports can be executed automatically (e.g. daily or monthly) or on demand from the **Reports** view.


PRTG Traffic Grapher - test.prtg
File Edit View Tags Extras Help
Views
View: Reports
Add Delete Edit View
Data
Events
Sensors
Custom
Reports
Browser
Name Period Detail Sensors Send Email Save to File Schedule
My Daily Report Day (00:00 - 23:59) 1 Day 3 dailyreport@company.com HTML every day at 00:00h
CEO's monthly report Month 1 Day 1 ceo@company.com every month on the 1. at 01:00h
PAESSLER
V7.1.0.217 Netflow Edition LocalDev
1445 refreshs
8% CPU Load

Please see the section Creating Reports for details.

Web Browser View

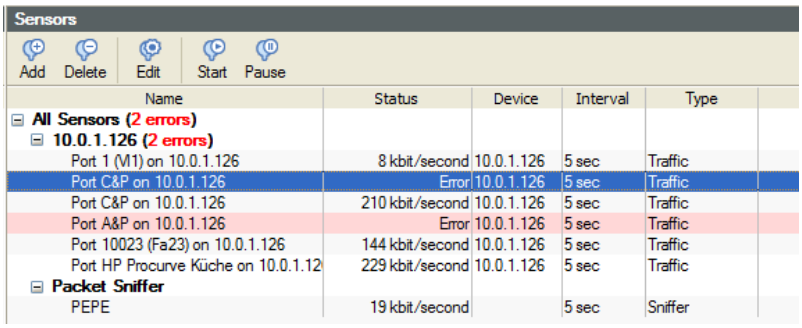
This view enables you to access the web interface of PRTG. The usage is the same as you are used from Internet Explorer.



Of course you can also access the web interface using a standard web browser. Right click on the URL to copy it or open the standard browser.

Working With Sensors

You can find the list of sensors in the middle of the main Window:



Name	Status	Device	Interval	Type
All Sensors (2 errors)				
10.0.1.126 (2 errors)				
Port 1 (V1) on 10.0.1.126	8 kbit/second	10.0.1.126	5 sec	Traffic
Port C&P on 10.0.1.126	Error	10.0.1.126	5 sec	Traffic
Port C&P on 10.0.1.126	210 kbit/second	10.0.1.126	5 sec	Traffic
Port A&P on 10.0.1.126	Error	10.0.1.126	5 sec	Traffic
Port 10023 (Fa23) on 10.0.1.126	144 kbit/second	10.0.1.126	5 sec	Traffic
Port HP Procurve Küche on 10.0.1.12	229 kbit/second	10.0.1.126	5 sec	Traffic
Packet Sniffer				
PEPE	19 kbit/second		5 sec	Sniffer

Each sensor in the list is shown with its name and the current reading, as well as the IP address, interval, sensor type, and comment.

Sensors that can not be accessed (e.g. due to misconfiguration, network problems, or outage of the device) are shown with a red background.

A yellow background symbolizes a paused state (paused by the user or by licensing).

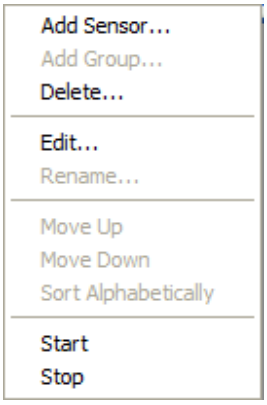
Using the toolbar you can add new sensors as well as delete or edit the existing sensors. Use **Start** and **Stop** to pause and resume monitoring of a sensor or a group.

Using drag&drop you can change the order of the sensors or drag a sensor from one group into another one. Use CTRL and SHIFT while clicking a sensor to select more than one sensor at once.

Double click a sensor to edit it. Editing the different sensor types is described a little later in this manual.

To edit the settings of several sensors at once select the sensors and click on **Edit**.

There is also a context menu for the sensors that enables you to work with the sensors:

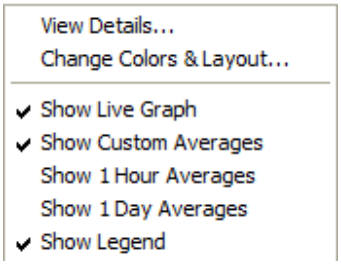


Working With Charts

Working with graphs is very similar in the Data and Custom views.

Graph Context Menu

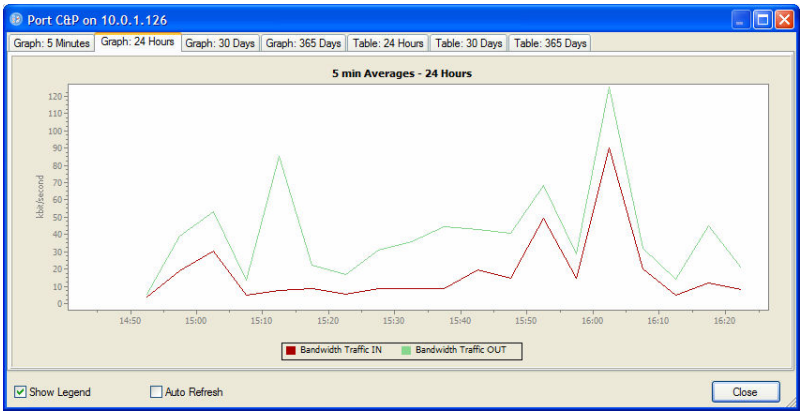
A right-click on a graph brings up a context menu that enables you to open the graph in its own window (**View Details,** see next section), change the colors and the layout. You can also select the graphs to show:



Graph Details Dialog

By double clicking a graph or by clicking the button, located on the top right side of the graph, it is possible to open the graph details dialog.

The **View Graph Details** dialog offers seven tabs – 4 for graph information and 3 for table information.



At the bottom of the window it is possible to define whether to show the legend or not and to enable auto-refreshing for the graphs (which can slow down the usage for graphs with many sensors).

The **Graph: 5 Minutes** tab displays standard graphing information for the last five minutes (according to the set interval).

The **Graph: 24 Hours** tab displays standard graphing information for the last 24 hours (in 5 minute averages).

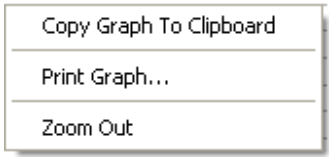
The **Graph: 30 days** tab displays standard graphing information for the last 30 days (in hourly averages).

The **Graph: 365 days** displays standard graphing information for the last year (in daily averages).

Zooming is done by dragging the mouse (while keeping the left mouse button down) from the top left to the bottom right of the region one wants to zoom in. To move the graph after zooming in click the graph with the right mouse button and keep the button pressed while moving the mouse.

In order to zoom out, one needs to drag the mouse from the bottom right to the top left of the region one wants to zoom out from.

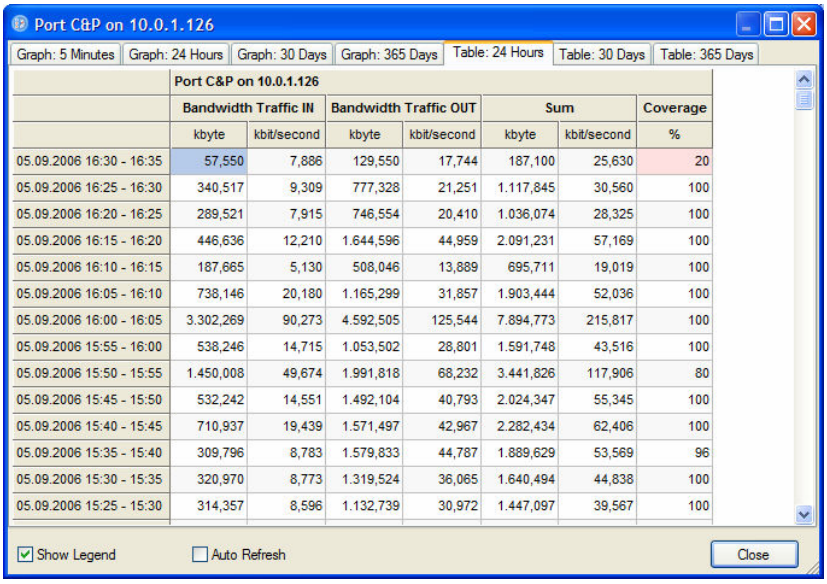
Each of these graphs is equipped with a right-click context menu. When right clicking on the appropriate table, a menu will appear.



Here, you have the option to copy the graph to the clipboard, print the graph, or zoom out. Zooming out, basically allows you to zoom back to the complete chart after zooming in.

Note: Copying the graph will also include the Legend information shown at the bottom of the graph.

The **Table: 24 Hours** tab displays a data table with the data for the last 24 hours.



Port C&P on 10.0.1.126							
	Bandwidth Traffic IN		Bandwidth Traffic OUT		Sum		Coverage
	kbyte	kbit/second	kbyte	kbit/second	kbyte	kbit/second	%
05.09.2006 16:30 - 16:35	57,550	7,886	129,550	17,744	187,100	25,630	20
05.09.2006 16:25 - 16:30	340,517	9,309	777,328	21,251	1.117,845	30,560	100
05.09.2006 16:20 - 16:25	289,521	7,915	746,554	20,410	1.036,074	28,325	100
05.09.2006 16:15 - 16:20	446,636	12,210	1.644,596	44,959	2.091,231	57,169	100
05.09.2006 16:10 - 16:15	187,665	5,130	508,046	13,889	695,711	19,019	100
05.09.2006 16:05 - 16:10	738,146	20,180	1.165,299	31,857	1.903,444	52,036	100
05.09.2006 16:00 - 16:05	3.302,269	90,273	4.592,505	125,544	7.894,773	215,817	100
05.09.2006 15:55 - 16:00	538,246	14,715	1.053,502	28,801	1.591,748	43,516	100
05.09.2006 15:50 - 15:55	1.450,008	49,674	1.991,818	68,232	3.441,826	117,906	80
05.09.2006 15:45 - 15:50	532,242	14,551	1.492,104	40,793	2.024,347	55,345	100
05.09.2006 15:40 - 15:45	710,937	19,439	1.571,497	42,967	2.282,434	62,406	100
05.09.2006 15:35 - 15:40	309,796	8,783	1.579,833	44,787	1.889,629	53,569	96
05.09.2006 15:30 - 15:35	320,970	8,773	1.319,524	36,065	1.640,494	44,838	100
05.09.2006 15:25 - 15:30	314,357	8,596	1.132,739	30,972	1.447,097	39,567	100

In the case of traffic sensors, information about the **Bandwidth Traffic IN**, the **Bandwidth Traffic OUT**, the **SUM** of the traffic, as well as the **coverage** value is included. This value tells you whether the monitoring was on all the time and covered the complete time period.

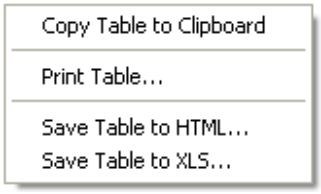
At the bottom of this graph you will find a section which represents the total sums and averages.

Totals for 04.09.2006 16:35 - 05.09.2006 16:35							
Total Volume	12.323,771		28.160,836		40.484,606		
Average	665,629	17,000	1.505,796	38,294	1.085,712	55,294	7

The **Table: 30 Days** tab, displays a table listing pertinent information, as regards the last 30 days.

The **Table: 365 Days** tab, displays a table listing pertinent information, as regards the last year.

Each of these tables is equipped with a right-click context menu. When right clicking on the appropriate table, a menu will appear.

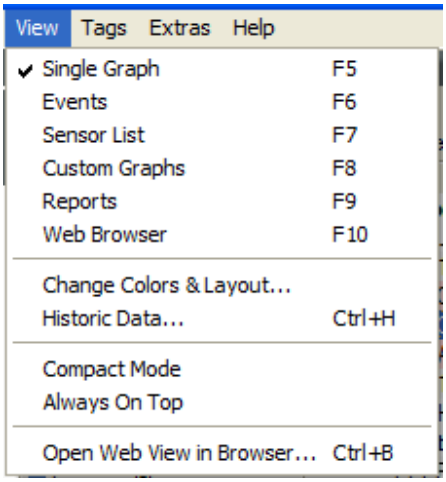


Here, you have the option to copy the information to the clipboard, print the table, save the table to an HTML file, or save the table as an XLS (Excel) data file.

When wishing to save the information (either as HTML or as XLS) a menu will open allowing you to select a directory where to save the respective data file.

Using the View Menu

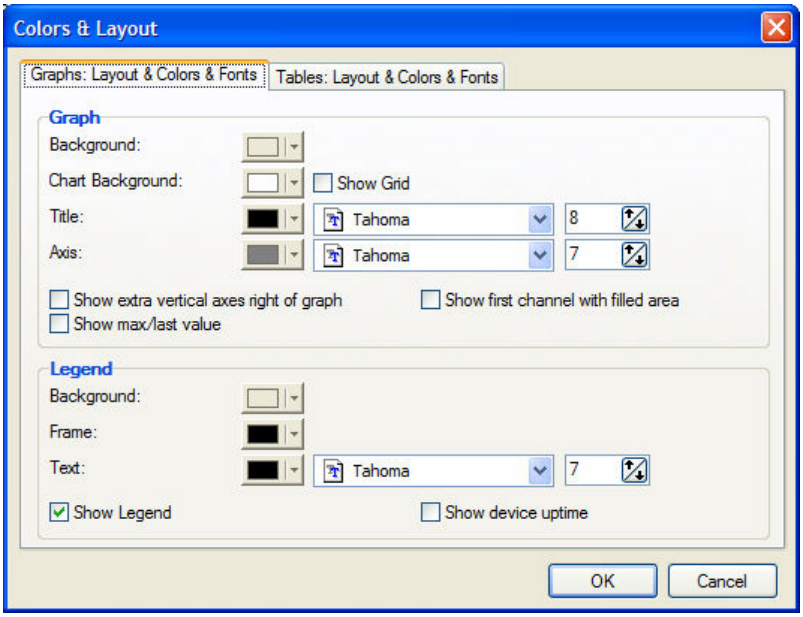
Clicking on the **View** option from the main menu will cause the **View** menu to drop down:



Here you can select the desired view, change the default colors&layouts of the graphs and view the historic data of a sensor.

Change Colors & Layout

Here you can edit the colors and the layout of the graphs and tables throughout the program and the web interface – except for the custom views which store their own settings.

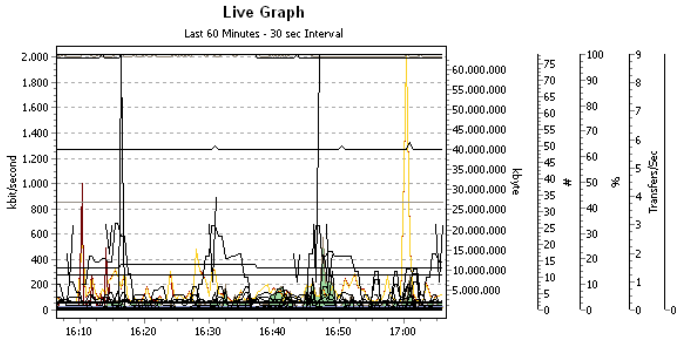


The first section, **Graph**, allows you to change the **Background** color, as well as selecting whether a **grid** is shown or not. Here, it is also possible to define the colors for the **Title** and **Axis** color.

Next to these controls, one can define the fonts used during the graph display, as well as their size. In order to change colors and fonts, click on the appropriate drop-down buttons and select the color and font you would like to see displayed with the graph. In order to change the size of the fonts, either click on the up and down arrows, in order to increase or decrease the font size, respectively, or merely enter the desired value in the field provided.

In the lower range of this section, you have a series of checkboxes which allow you to affect the way the graph is displayed. Checking the appropriate checkboxes, you can activate / deactivate the following functions:

- **Show extra vertical axes right of graph** – if sensors with more than 2 different vertical units are shown in one graph, this option will enable displaying all axis on the right side with the specified units. This can sometimes take a lot of space and is not enabled by default.
  Here is a sample:



- **Show max/last value** – this will display the maximum and the last measured value below a graph. Here is a sample:

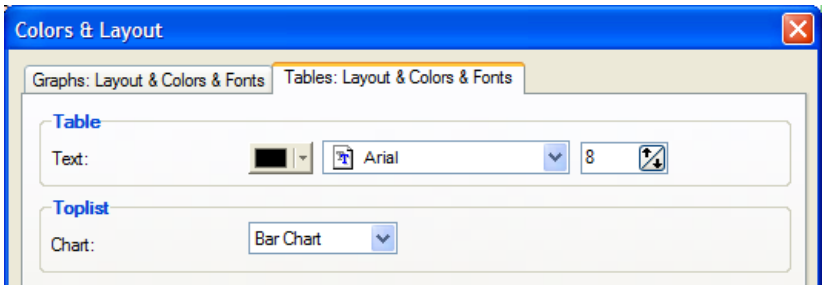
  Bandwidth Traffic OUT: Max=839,438, Last=8,612 [kbit/second]
  Bandwidth Traffic IN: Max=2.072,09, Last=65,223 [kbit/second]

- **Show first sensor with filled area** – this will enable the graph for the first sensor to be displayed with a filled area, making it easier to judge the graph information.

In the **Legend** section you can change the look and information of the legend shown below the graphs. Here, you are able to define colors for the background, the frame, and the text that appears in the legend. You can also define a font for the text, as well as its size.

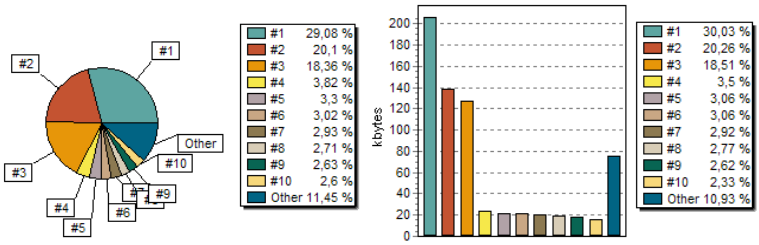
In order for the legend to be displayed, the **Show Legend** checkbox has to be selected.

The **Show device uptime** checkbox can be selected in order to have the uptime of each device (i.e. the time since the last reboot) shown in the legend area.



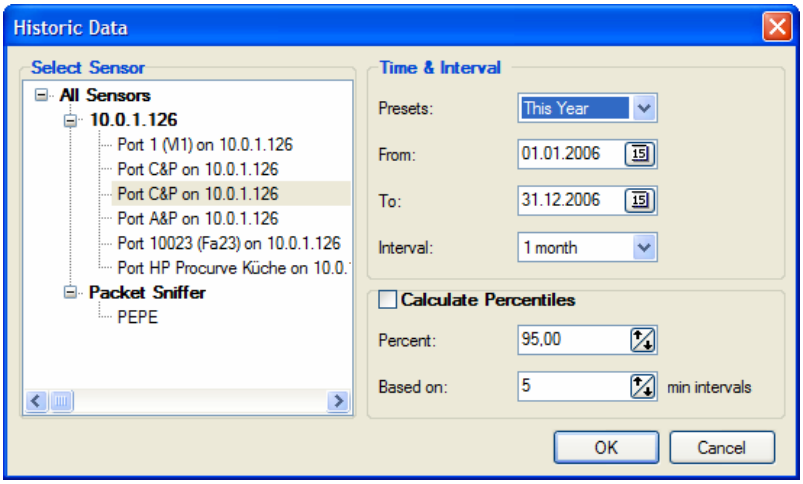
In the panel **Tables: Layout & Colors & Fonts** you can finally control how the tables are shown.

Under **Toplist** you can choose whether to show the **charts** for the toplists as **bar chart** or **pie chart** – or select **none** to disable charts for toplists.



View Historic Data

With this menu item you can access the data in PRTG's monitoring database.



Please select a sensor on the left. In the **Time&Interval** section you can define the report parameters.

Select a preset for the time lapse for which the report is to be generated or select a time period by entering specific start and end dates.

Please choose a Preset or you can also enter **From** and **To** dates manually, then the **Time Frame Presets** mode will automatically switch to **Custom**. Also please choose an **Interval**.

At the bottom of the window, one can activate the percentile calculation setting (only available when using delta sensors, e.g. Traffic sensors). Here you can define the percentage to be used, as well as the time interval the calculation is to be based on.

Upon clicking **OK**, the report is generated and displayed.

The report is generated both as a graph and as a table, the view of which can be selected by pressing the appropriate tab.

Click on **Edit** to change the channels, colors, etc. This is the same dialog as all "detailed graphs" windows offer.

Compact Mode and Always On Top

View|Compact Mode will remove the toolbar, as well as other GUI information. Only the sensor list and the panels will remain.

Always on Top will cause PRTG Traffic Grapher to remain "on top", i.e. over any other window you might be working with.

A combination of **Compact Mode** and **Always on Top** allows you - when the window is reduced – to move the PRTG window to a corner of your screen to be visible, without being obtrusive. Also note that the PRTG Traffic Grapher window will "snap" to a position, when brought to the edge of the active monitor area.

Open Web View in Browser

Choose this menu item to open your standard web browser with the homepage of PRTG's web interface.

Adding Sensors

Available Sensor Types

To monitor bandwidth usage, PRTG offers the four common data acquisition methods:

- SNMP
- Packet Sniffing
- NetFlow
- Latency
- Sensor Aggregation

See "SNMP Monitoring" for more details about these options.

Adding SNMP Sensors

Choosing between Standard Traffic, SNMP Helper, Library, or Custom SNMP Sensors

PRTG Traffic Grapher offers several types of SNMP sensors:

Standard Traffic Sensor: This is the most common usage of SNMP. Via the MIB-2 standard PRTG can access the traffic counters of a device to monitor its bandwidth.

SNMP Helper Sensor: Paessler SNMP Helper is a system-level software program that runs on a Windows 2000, XP, or 2003 computer system that allows other systems running PRTG Traffic Grapher to collect performance information remotely for several thousand Windows Performance Counters, using the SNMP protocol. See the section "Paessler SNMP Helper" for more details.

From OID/MIB Library: PRTG comes with several preconfigured libraries (so called "OIDLIBs") for various device types that helps you to monitor CPU loads, disk usage, or temperatures. Additionally you can convert most MIB files from device vendors into OIDLIBs using Paessler's MIB Import Tool to create many more sensors. See the section "Importing MIBs using Paessler MIB Importer and Converter" for more details.

Custom SNMP sensors: Choose this type if you want to monitor an SNMP OID value that PRTG does not have built into its libraries. You must supply the OID value for the reading you want to monitor.

Device Template: You can create your own device templates. A device template can be use to create the same set of sensors for a number of devices. See the section Working with Device Templates.

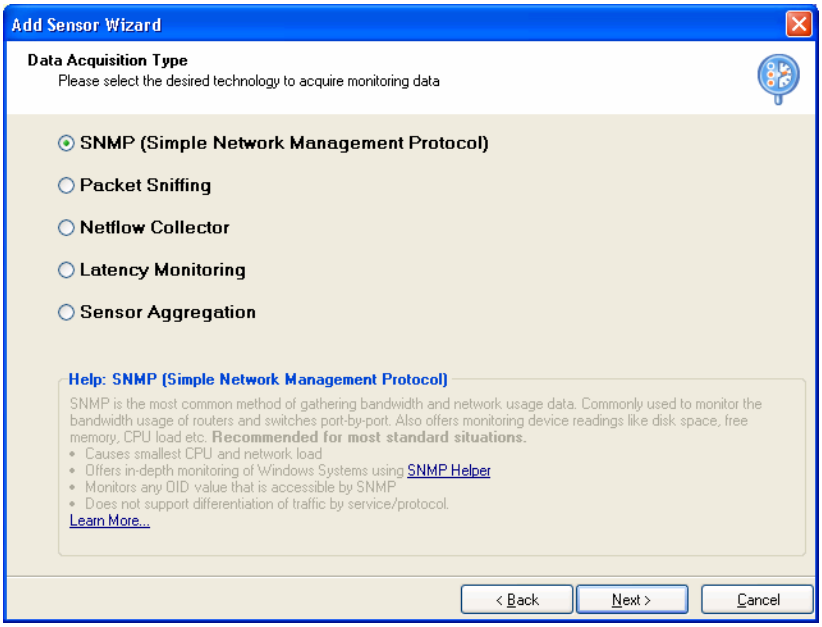
All SNMP Sensor Types: Starting the Add Sensor Wizard

In order to add a new sensor, click on the **Add Sensor** button in the sensor list's toolbar or select **Add New Sensor** from the **Edit** menu.

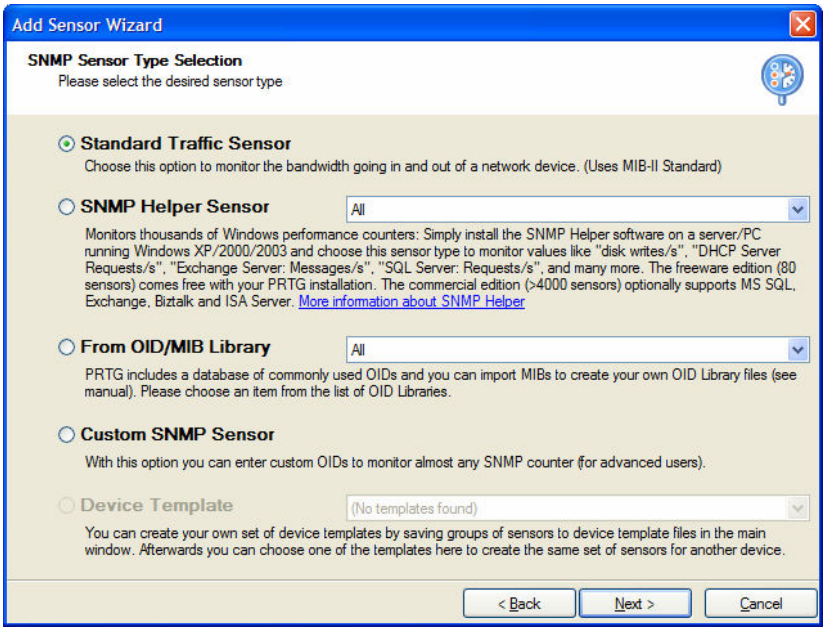
This will launch the **Add Sensor Wizard**.

Add Sensor Wizard
Welcome to the Add Sensor Wizard
This wizard will guide you step-by-step through the setup of new sensors for monitoring with PRTG Traffic Grapher.
Creating new sensors involves three main steps:
1. Selecting the data acquisition technology (SNMP, packet sniffing or NetFlow)
2. Selecting the device/server and scanning it for available sensors
3. Selecting the new sensors and choosing a group as well as an interval
Note: If you want PRTG Traffic Grapher to scan your network automatically for SNMP enabled devices please use the Automatic Network Discovery to create SNMP based sensors.
Please click "Next" to continue!
PAESSLER
< Back
Next >
Cancel

Click **Next** to proceed to the selection of the data acquisition.


Add Sensor Wizard
Data Acquisition Type
Please select the desired technology to acquire monitoring data
SNMP (Simple Network Management Protocol)
Packet Sniffing
Netflow Collector
Latency Monitoring
Sensor Aggregation
Help: SNMP (Simple Network Management Protocol)
SNMP is the most common method of gathering bandwidth and network usage data. Commonly used to monitor the bandwidth usage of routers and switches port-by-port. Also offers monitoring device readings like disk space, free memory, CPU load etc. Recommended for most standard situations.
Causes smallest CPU and network load
Offers in-depth monitoring of Windows Systems using SNMP Helper
Monitors any OID value that is accessible by SNMP
Does not support differentiation of traffic by service/protocol.
Learn More...
< Back
Next >
Cancel

Please select **SNMP** and click **Next**. This will lead to the SNMP Sensor Selection page:


Add Sensor Wizard
SNMP Sensor Type Selection
Please select the desired sensor type
Standard Traffic Sensor
Choose this option to monitor the bandwidth going in and out of a network device. (Uses MIB-II Standard)
SNMP Helper Sensor
All
Monitors thousands of Windows performance counters: Simply install the SNMP Helper software on a server/PC running Windows XP/2000/2003 and choose this sensor type to monitor values like "disk writes/s", "DHCP Server Requests/s", "Exchange Server: Messages/s", "SQL Server: Requests/s", and many more. The freeware edition (80 sensors) comes free with your PRTG installation. The commercial edition (>4000 sensors) optionally supports MS SQL, Exchange, Biztalk and ISA Server. More information about SNMP Helper
From OID/MIB Library
All
PRTG includes a database of commonly used OIDs and you can import MIBs to create your own OID Library files (see manual). Please choose an item from the list of OID Libraries.
Custom SNMP Sensor
With this option you can enter custom OIDs to monitor almost any SNMP counter (for advanced users).
Device Template
(No templates found)
You can create your own set of device templates by saving groups of sensors to device template files in the main window. Afterwards you can choose one of the templates here to create the same set of sensors for another device.
< Back
Next >
Cancel

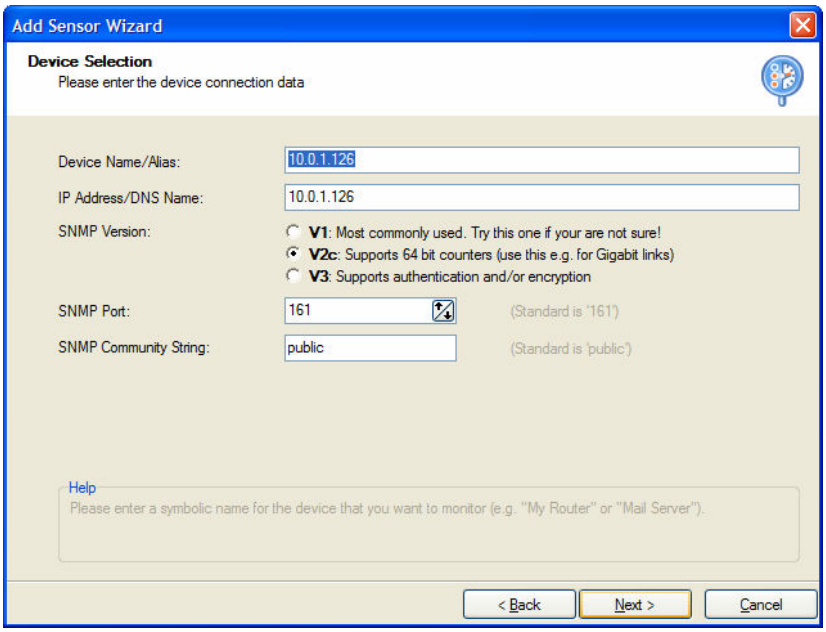
For **SNMP Helper Sensors** and **OIB/MIB Library Sensors** you can either leave the selection in the dropdown to "All", which will cause PRTG to scan the device with all available libraries and can take some time. Or you can specifically choose on of the entries.

For more Information about SNMP Helper and OIDLIBs please see the sections "Paessler SNMP Helper" and "Importing MIBs using Paessler MIB Importer and Converter".

The individual types of sensors are discussed below. Please choose the desired type and click **Next**.

All SNMP Sensor Types: Device Selection

After choosing the SNMP Sensor type clicking the **Next** button will bring up the **Device Selection** window.


Add Sensor Wizard
Device Selection
Please enter the device connection data
Device Name/Alias:
10.0.1.126
IP Address/DNS Name:
10.0.1.126
SNMP Version:
V1: Most commonly used. Try this one if your are not sure!
V2c: Supports 64 bit counters (use this e.g. for Gigabit links)
V3: Supports authentication and/or encryption
SNMP Port:
161
(Standard is '161')
SNMP Community String:
public
(Standard is 'public')
Help
Please enter a symbolic name for the device that you want to monitor (e.g. "My Router" or "Mail Server").
< Back
Next >
Cancel

In the **Device Selection** window, you have the options to enter the following information:

- **Device Name / Alias**
- **IP Address / DNS Name**
- **SNMP Version**
- **SNMP Port**
- **SNMP Community String** or **Account Information**

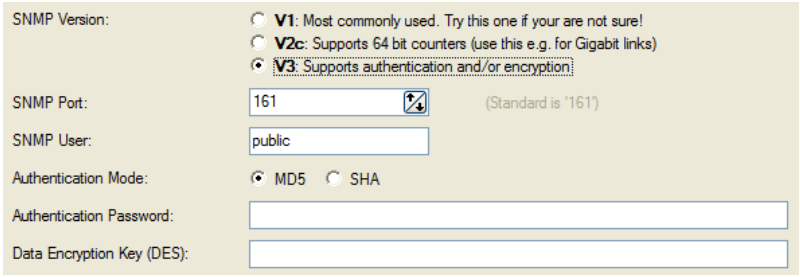
In the **Device Name / Alias** field, you can enter the desired name with which to identify this device.

In the **IP address / DNS name** field, please enter the specific IP address (e.g. 10.0.0.1) / DNS name (e.g. router.corp.com) for the device you would like to monitor. Make sure that the information entered is accurate, as otherwise PRTG Traffic Grapher will not be able to access the device.

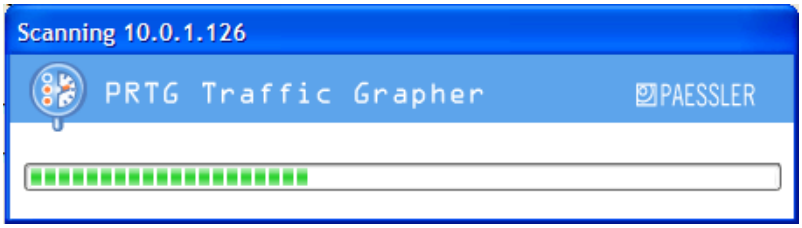
In the **SNMP Port** field define the port number for the device you want to monitor. You can use the arrow keys to change the value or you can enter it directly in the field provided. The standard (default) value is 161.

In the **SNMP Community String** field (only for SNMP V1 and 2c), enter the information required for the community string, in order to allow PRTG Traffic Grapher to access the device. The standard, default value for this is “public”.

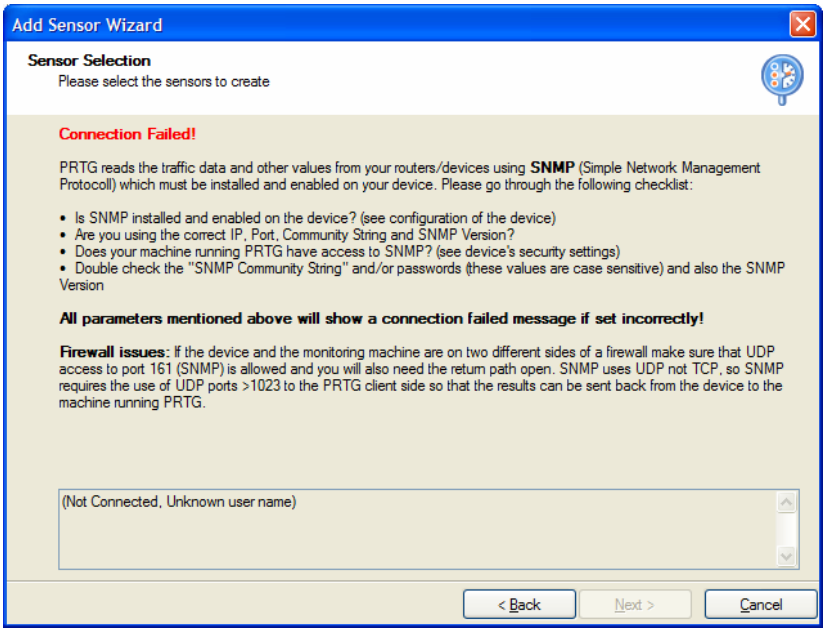
If you are using SNMP V3 you also have to the **SNMP User**, **Authentication Mode** and **Password** as well as the optional **Data Encryption** key.



Click **Next** to continue. Now PRTG Traffic Grapher tries to contact the device for the first time.



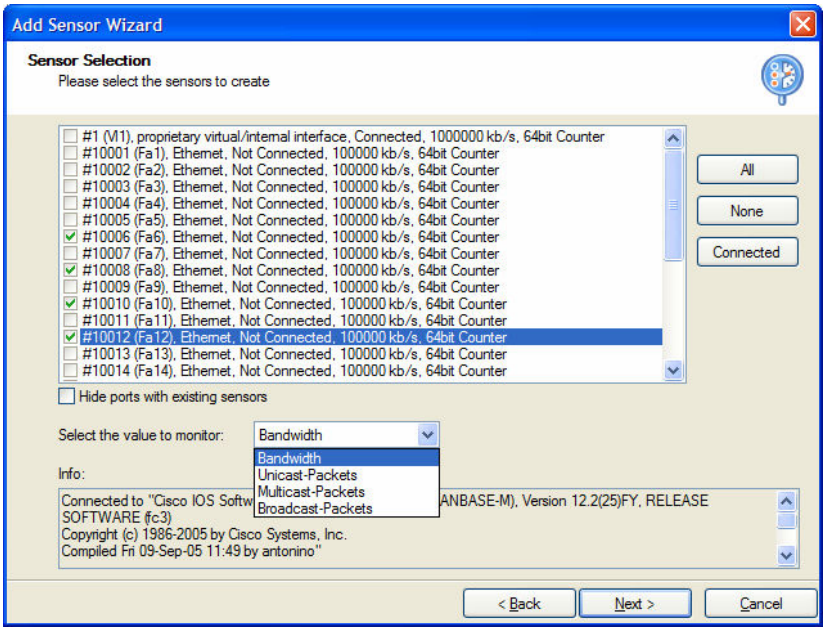
If the connection fails you will get an error message. In this case, please follow the instructions on the screen!


Add Sensor Wizard
Sensor Selection
Please select the sensors to create
Connection Failed!
PRTG reads the traffic data and other values from your routers/devices using SNMP (Simple Network Management Protocol) which must be installed and enabled on your device. Please go through the following checklist:
• Is SNMP installed and enabled on the device? (see configuration of the device)
• Are you using the correct IP, Port, Community String and SNMP Version?
• Does your machine running PRTG have access to SNMP? (see device's security settings)
• Double check the "SNMP Community String" and/or passwords (these values are case sensitive) and also the SNMP Version
All parameters mentioned above will show a connection failed message if set incorrectly!
Firewall issues: If the device and the monitoring machine are on two different sides of a firewall make sure that UDP access to port 161 (SNMP) is allowed and you will also need the return path open. SNMP uses UDP not TCP, so SNMP requires the use of UDP ports >1023 to the PRTG client side so that the results can be sent back from the device to the machine running PRTG.
(Not Connected, Unknown user name)
< Back
Next >
Cancel

Depending on the type of SNMP sensor you have chosen above please refer to the corresponding sections below.

SNMP Traffic Sensors: Port Selection

After entering the device's IP address in the Add Sensor Wizard clicking the **Next** button will bring up the **Port Selection** window.


Add Sensor Wizard
Sensor Selection
Please select the sensors to create
#1 (V1), proprietary virtual/internal interface, Connected, 1000000 kb/s, 64bit Counter
#10001 (Fa1), Ethernet, Not Connected, 100000 kb/s, 64bit Counter
#10002 (Fa2), Ethernet, Not Connected, 100000 kb/s, 64bit Counter
#10003 (Fa3), Ethernet, Not Connected, 100000 kb/s, 64bit Counter
#10004 (Fa4), Ethernet, Not Connected, 100000 kb/s, 64bit Counter
#10005 (Fa5), Ethernet, Not Connected, 100000 kb/s, 64bit Counter
#10006 (Fa6), Ethernet, Not Connected, 100000 kb/s, 64bit Counter
#10007 (Fa7), Ethernet, Not Connected, 100000 kb/s, 64bit Counter
#10008 (Fa8), Ethernet, Not Connected, 100000 kb/s, 64bit Counter
#10009 (Fa9), Ethernet, Not Connected, 100000 kb/s, 64bit Counter
#10010 (Fa10), Ethernet, Not Connected, 100000 kb/s, 64bit Counter
#10011 (Fa11), Ethernet, Not Connected, 100000 kb/s, 64bit Counter
#10012 (Fa12), Ethernet, Not Connected, 100000 kb/s, 64bit Counter
#10013 (Fa13), Ethernet, Not Connected, 100000 kb/s, 64bit Counter
#10014 (Fa14), Ethernet, Not Connected, 100000 kb/s, 64bit Counter
All
None
Connected
Hide ports with existing sensors
Select the value to monitor:
Bandwidth
Bandwidth
Unicast-Packets
Multicast-Packets
Broadcast-Packets
Info:
Connected to "Cisco IOS Softw
ANBASE-M), Version 12.2(25)FY, RELEASE
SOFTWARE (fc3)
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Fri 09-Sep-05 11:49 by antonino"
< Back
Next >
Cancel

In the **Port Selection** window you will find a listing of all the defined device's ports that can be monitored. Here, you can select any number of ports to be monitored. In order to select a port check the checkbox before the port definition.

The shortcut buttons **All**, **None**, and **Connected** (all ports that currently have a connection) can also be used to select ports. Clicking the **Hide ports with existing sensors** checkbox will remove all ports that have already a sensor from the list to prevent duplicate monitoring.

At the bottom of this window, you will find a drop-down menu that allows you to define what kind of value you want to monitor.

For 32bit counters the options are:

- **Bandwidth**
- Number of **Unicast Packets**
- Number of **Non-Unicast Packets**
- Number of **Errors**

For 64bit counters:

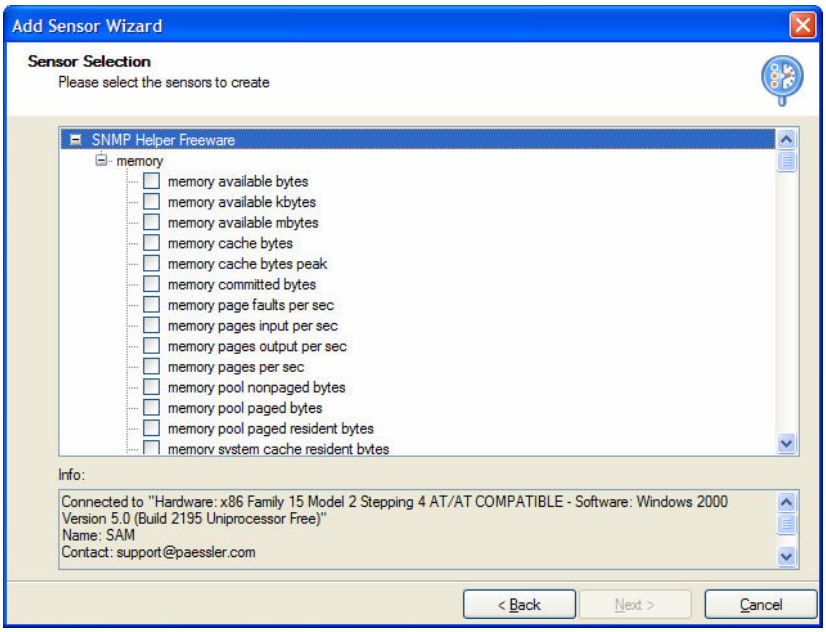
- **Bandwidth**
- Number of **Unicast Packets**
- Number of **Multicast Packets**
- Number of **Broadcast Packets**

Advanced Tip: If you prefer to use 32bit counters with SNMP V3 (e.g. to get the error counters) you can activate the **Force 32bit traffic counters** option in the advanced high compatibility mode on the **tweaks** page of the options, otherwise SNMP V3 will always use 64bit counters.

Once you have made your desired settings for the new SNMP sensor click on the **Next** button. This will bring up the **Additional Settings** window.

SNMP Helper Sensors: Sensor Selection

After entering the device's IP address in the Add Sensor Wizard clicking the **Next** button will bring up the **Sensor Selection** window.

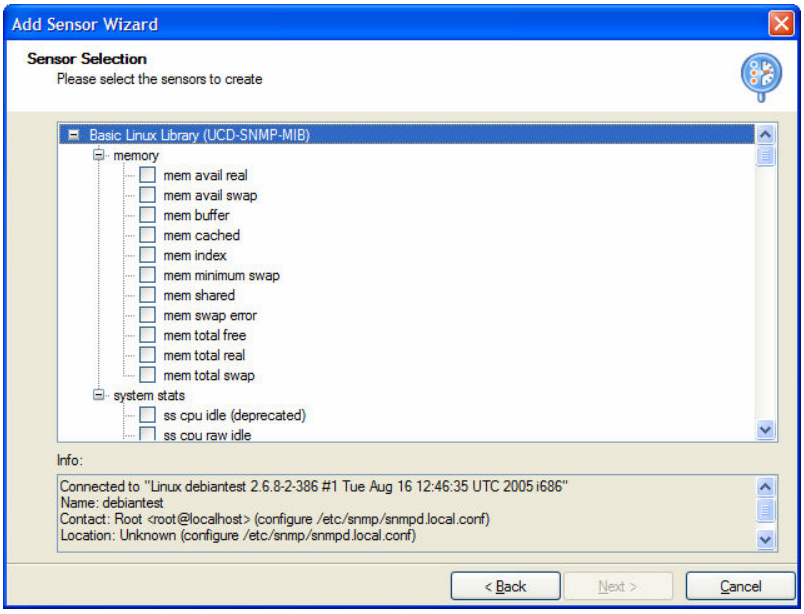

Add Sensor Wizard
Sensor Selection
Please select the sensors to create
SNMP Helper Freeware
memory
memory available bytes
memory available kbytes
memory available mbytes
memory cache bytes
memory cache bytes peak
memory committed bytes
memory page faults per sec
memory pages input per sec
memory pages output per sec
memory pages per sec
memory pool nonpaged bytes
memory pool paged bytes
memory pool paged resident bytes
memory system cache resident bytes
Info:
Connected to "Hardware: x86 Family 15 Model 2 Stepping 4 AT/AT COMPATIBLE - Software: Windows 2000 Version 5.0 (Build 2195 Uniprocessor Free)"
Name: SAM
Contact: support@paessler.com
< Back
Next >
Cancel

In this window you will find a tree listing of all of the readings that PRTG has found on the device and that can be monitored. Here, you can select any number of entries to be monitored. In order to select an entry, unfold the relevant tree branch and check the checkbox in front of the desired entries (one or more).

Once you have made your selections, click on the **Next** button. This will bring up the **Additional Settings** window.

OIDLIB/MIB Library Sensors: Sensor Selection

After entering the device's IP address in the Add Sensor Wizard clicking the **Next** button will bring up the **Port Sensor** window.



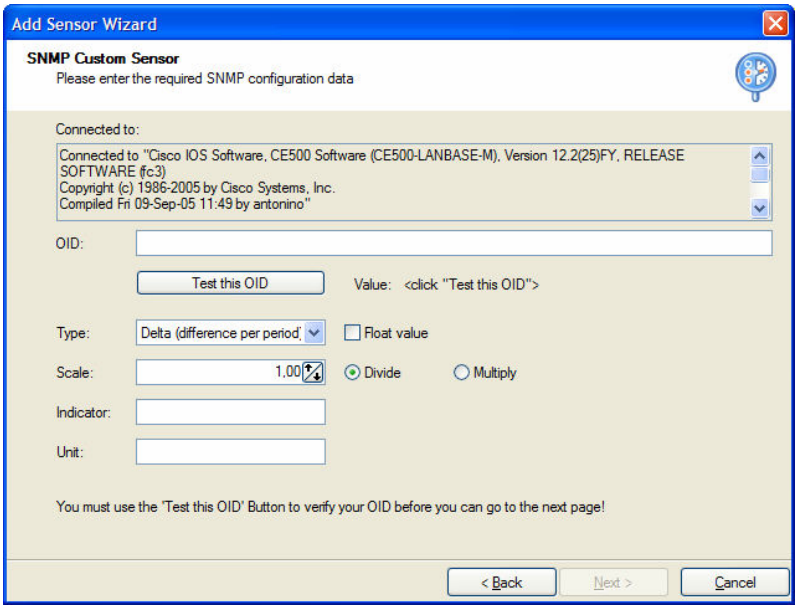
In this window you will find a tree listing of all of the readings that PRTG has found on the device and that can be monitored. Here, you can select any number of entries to be monitored. In order to select an entry, unfold the relevant tree branch and check the checkbox in front of the desired entries (one or more).

Once you have made your selections, click on the **Next** button. This will bring up the **Additional Settings** window.

Custom SNMP Sensors: OID Entry

Note: In order to set up custom OIDs you must know the OID code of the value you want to monitor. If you do not know the OID value already you may need to find it out using an SNMP Walker.

After entering the device's IP address in the Add Sensor Wizard clicking the **Next** button will bring up the SNMP **Custom Sensor** window.



First you have to enter an OID. OID (Object IDentifiers) are number codes used by SNMP to identify specific readings. They usually look like this: “1.2.3.4.5.6.7.8”. Please remove any leading “.”.

In order to test the OID for validity you have to click on the **Test this OID** button to continue. If the OID is valid, the value on the right-hand side will change from **<click “Test this OID”>** to a numerical value.

You can then define the type of measuring you want to do. Your options are:

- **Gauge (absolute value)**
- **Delta (difference per period)**

Check the **Float value** box if the returned value is a float (with a decimal point).

The **Scale** function is a floating point value through which the value delivered from the SNMP sensor is either divided or multiplied. You can select which one of the two to perform by clicking on the appropriate radio button to the right.

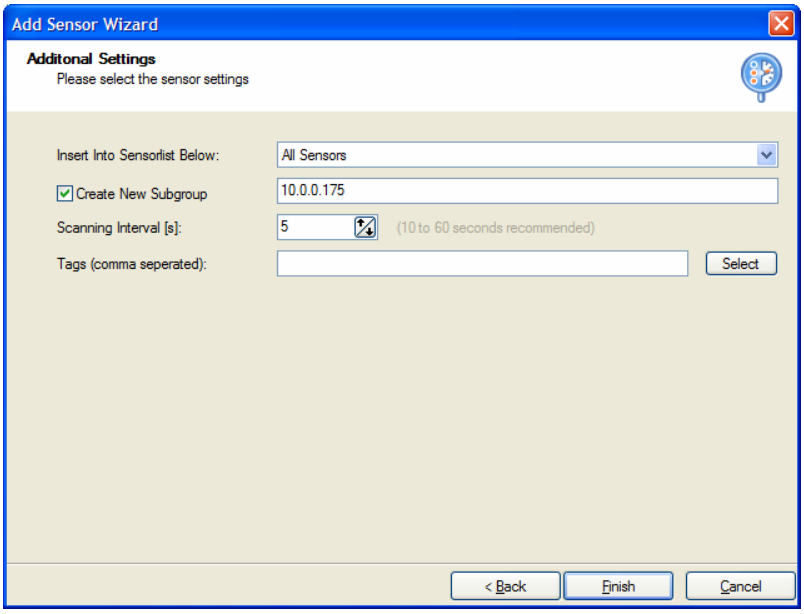
The **Indicator** field can be used to enter information that will be shown in the legend, as the name for the information of the sensor.

In the **Unit** field you can enter any string that shall be used as units when displaying the graphs.

Once you have made your selections, click on the **Next** button. This will bring up the **Additional Settings** window.

All SNMP Sensor Types: Additional Settings

Once you have made your desired settings for the new SNMP sensor click on the **Next** button. This will bring up the **Additional Settings** window.



Choose a group from the sensor list that you want to add the new sensor(s) to. Optionally you can **Create a New Subgroup**.

Choose a group name that will help you to keep your sensors organized (e.g. "Firewall" or "LAN"). Also select the desired **scanning interval** in seconds. In most cases 30 seconds should be fine. For installation with hundreds or even thousands of sensors it is recommended to increase the interval to 5-15 minutes to minimize system load.

Finally you can add tags for the new sensors which will help you to categorize your sensors later. A tag consists of one or more words, e.g. switch, printer, 1st floor, 2nd floor, remote office, data center 1, data center 2, etc. Use commas to separate tags.When you are finished selecting your options, click on **Finish**. This will finish setting up the sensor and will start the monitoring of the sensor.

Adding Packet Sniffer Sensors

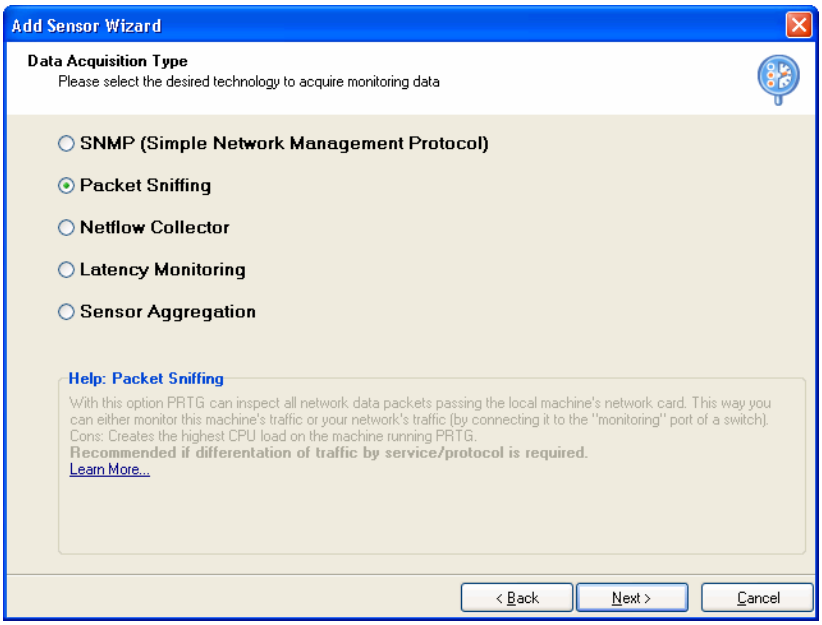
Starting the Add Sensor Wizard

In order to add a new sensor, click on the **Add Sensor** button in the sensor list's toolbar or select **Add New Sensor** from the **Edit** menu.

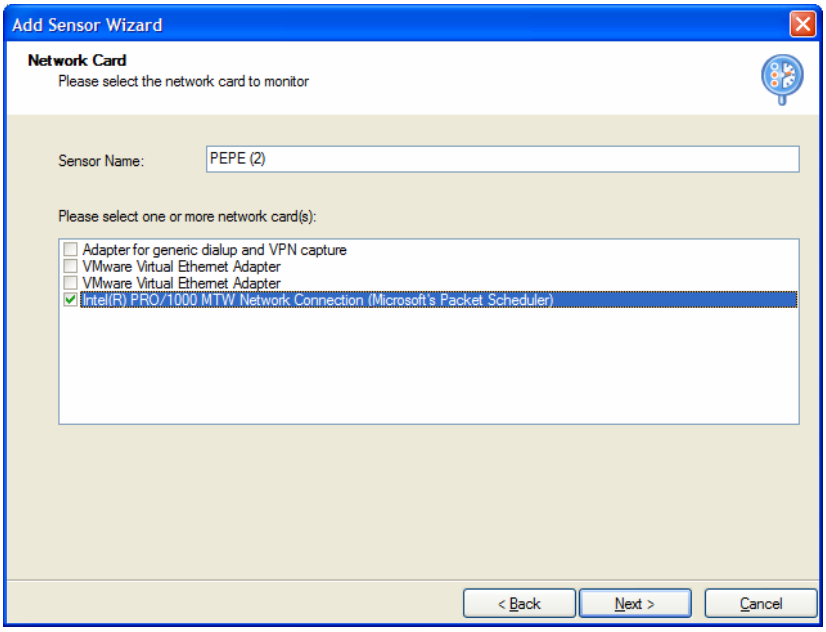
This will launch the **Add Sensor Wizard**.

Add Sensor Wizard
Welcome to the Add Sensor Wizard
This wizard will guide you step-by-step through the setup of new sensors for monitoring with PRTG Traffic Grapher.
Creating new sensors involves three main steps:
1. Selecting the data acquisition technology (SNMP, packet sniffing or NetFlow)
2. Selecting the device/server and scanning it for available sensors
3. Selecting the new sensors and choosing a group as well as an interval
Note: If you want PRTG Traffic Grapher to scan your network automatically for SNMP enabled devices please use the Automatic Network Discovery to create SNMP based sensors.
Please click "Next" to continue!
PAESSLER
< Back
Next >
Cancel

Click **Next** to proceed to the selection of the data acquisition.

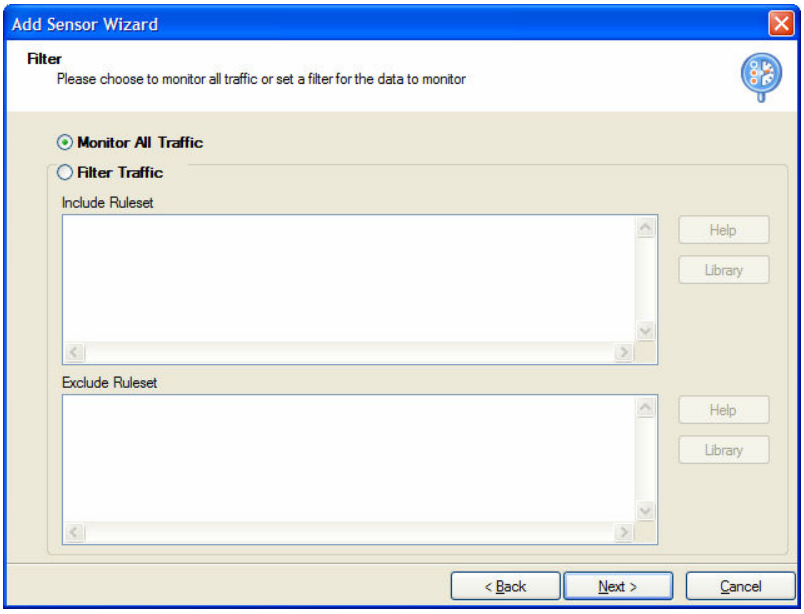

Add Sensor Wizard
Data Acquisition Type
Please select the desired technology to acquire monitoring data
SNMP (Simple Network Management Protocol)
Packet Sniffing
Netflow Collector
Latency Monitoring
Sensor Aggregation
Help: Packet Sniffing
With this option PRTG can inspect all network data packets passing the local machine's network card. This way you can either monitor this machine's traffic or your network's traffic (by connecting it to the "monitoring" port of a switch).
Cons: Creates the highest CPU load on the machine running PRTG.
Recommended if differentation of traffic by service/protocol is required.
Learn More...
< Back
Next >
Cancel

Please select **Packet Sniffing** and click **Next**. This will lead to the **Network Card** selection screen:


Add Sensor Wizard
Network Card
Please select the network card to monitor
Sensor Name:
PEPE (2)
Please select one or more network card(s):
Adapter for generic dialup and VPN capture
VMware Virtual Ethernet Adapter
VMware Virtual Ethernet Adapter
Intel(R) PRO/1000 MTW Network Connection (Microsoft's Packet Scheduler)
< Back
Next >
Cancel

From the list, choose the network card(s) you want to monitor (one or more). Then click the **Next** button. This will open the **Filter** window:

Filter Setup



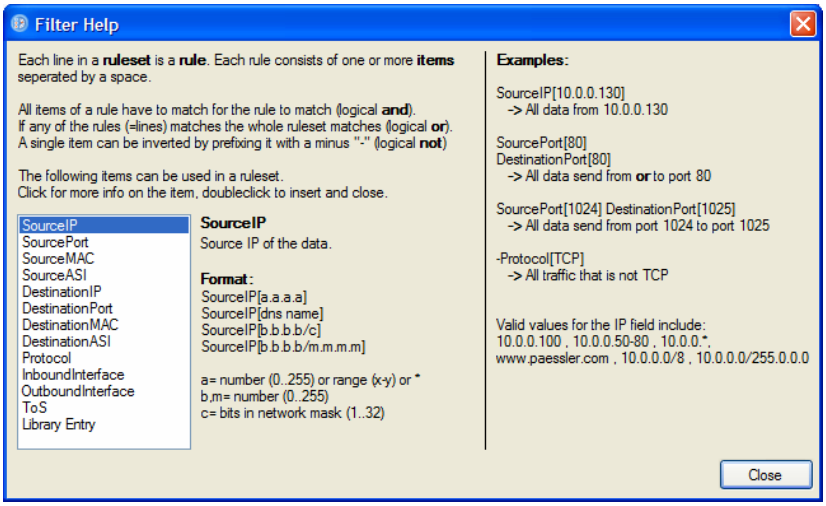
Here you can, first of all, select to **Monitor All Traffic** that passes through this device (default setting). The other option is to **Filter Traffic** by various parameters.

Note: Filtering traffic can become quite complex and is only recommended for experienced users. For most users simply choosing **Monitor All Traffic** should be fine.

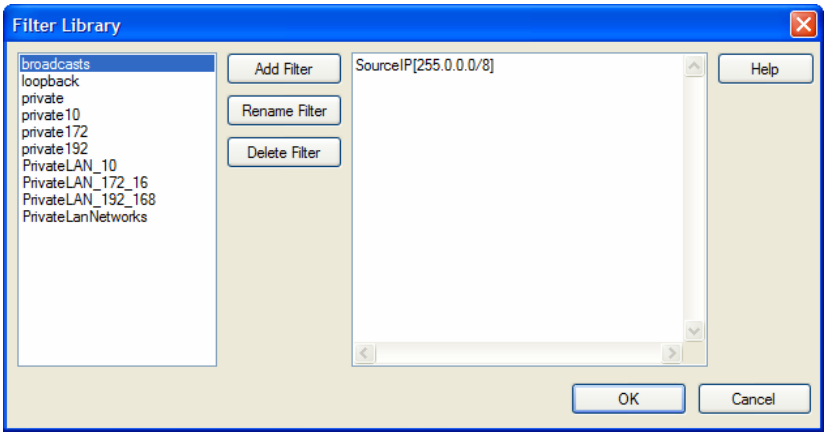
When enabling filtering you must supply two rulesets for inclusion and exclusion of traffic. For this reason the window is divided into two sections – **Include Ruleset** and **Exclude Ruleset**.

Include means that data packets that meet the settings of this filter will be included in PRTG's monitoring – as long as they are not filtered by an **Exclude** rule.

Click on **Help** for detailed description of the various rules that can be used:


Filter Help
Each line in a ruleset is a rule. Each rule consists of one or more items seperated by a space.
All items of a rule have to match for the rule to match (logical and).
If any of the rules (=lines) matches the whole ruleset matches (logical or).
A single item can be inverted by prefixing it with a minus "-" (logical not)
The following items can be used in a ruleset.
Click for more info on the item, doubleclick to insert and close.
SourceIP
SourcePort
SourceMAC
SourceASI
DestinationIP
DestinationPort
DestinationMAC
DestinationASI
Protocol
InboundInterface
OutboundInterface
ToS
Library Entry
SourceIP
Source IP of the data.
Format:
SourceIP[a.a.a.a]
SourceIP[dns name]
SourceIP[b.b.b.b/c]
SourceIP[b.b.b.b/m.m.m.m]
a= number (0..255) or range (x-y) or *
b,m= number (0..255)
c= bits in network mask (1..32)
Examples:
SourceIP[10.0.0.130]
-> All data from 10.0.0.130
SourcePort[80]
DestinationPort[80]
-> All data send from or to port 80
SourcePort[1024] DestinationPort[1025]
-> All data send from port 1024 to port 1025
-Protocol[TCP]
-> All traffic that is not TCP
Valid values for the IP field include:
10.0.0.100 , 10.0.0.50-80 , 10.0.0.*,
www.paessler.com , 10.0.0.0/8 , 10.0.0.0/255.0.0.0
Close

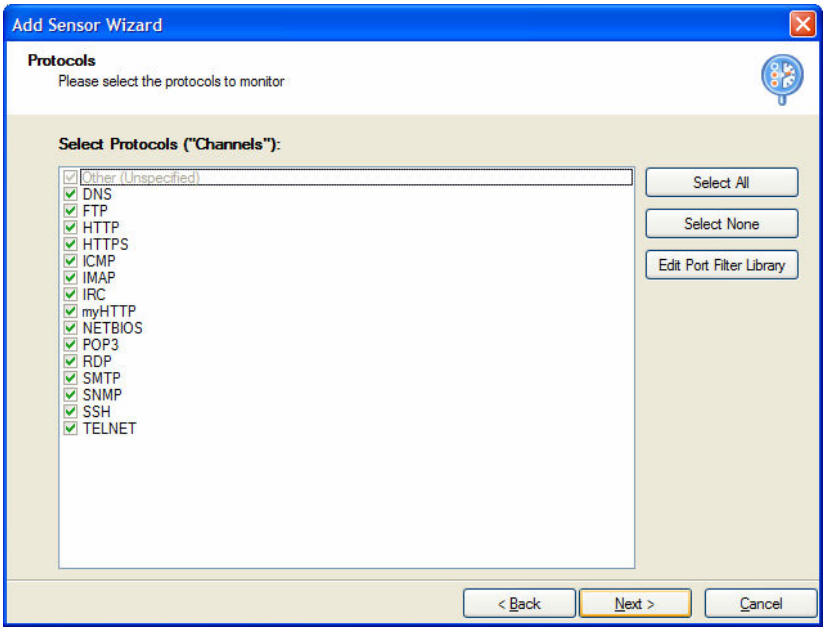
You can also click on Library to choose an item from the filter library:



Note: The items from the **Filter Library** can be edited using the **Extras** menu.

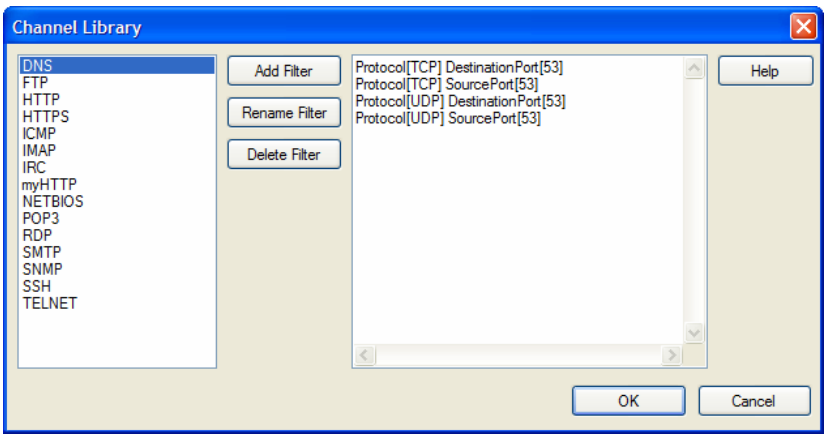
Click **Next** in order to go to the Protocol selection screen:

Protocol Setup



Here, you can select what protocols to monitor. Check the checkbox(es) of the protocol(s) you want to monitor or use the buttons on the right in order to **Select All** or **Select None**.

The **Edit Port Filter Library** button allows you to enter the port specification window.

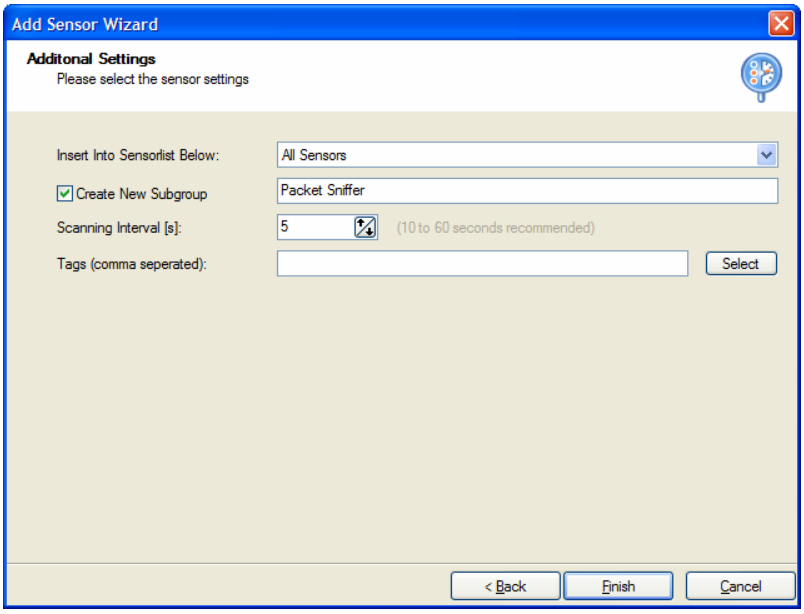


Here you can add a filter, rename a filter, or delete a filter, as well as add, edit, or delete a specificchannel.

Note: The items of the **Channel Library** can be edited using the **Extras** menu.

Additional Settings

Once you have made your desired settings for the new SNMP sensor click on the **Next** button. This will bring up the **Additional Settings** window.



Choose a group from the sensor list that you want to add the new sensor(s) to. Optionally you can **Create a New Subgroup**.

Choose a group name that will help you to keep your sensors organized (e.g. "Firewall" or "LAN"). Also select the desired **scanning interval** in seconds. In most cases 30 seconds should be fine. Since packet sniffing is a "push" technology, this value is only important for the screen update.

Finally you can add tags for the new sensors which will help you to categorize your sensors later. A tag consists of one or more words, e.g. switch, printer, 1st floor, 2nd floor, remote office, data center 1, data center 2, etc. Use commas to separate tags.

When you are finished selecting your options, click on **Finish**. This will finish setting up the sensor and will start the monitoring of the sensor.

NetFlow Sensors

Note 1: In order to use NetFlow sensors you must run a license that includes NetFlow monitoring. For each device that you want to monitor you need an individual NetFlow Collector.

- The NetFlow Edition of PRTG Traffic Grapher includes a number of NetFlow Collectors
- The Enterprise Licenses of PRTG Traffic Grapher can be upgraded with NetFlow Collector add-on licenses
- The Free Trial License includes 2 NetFlow sensors.

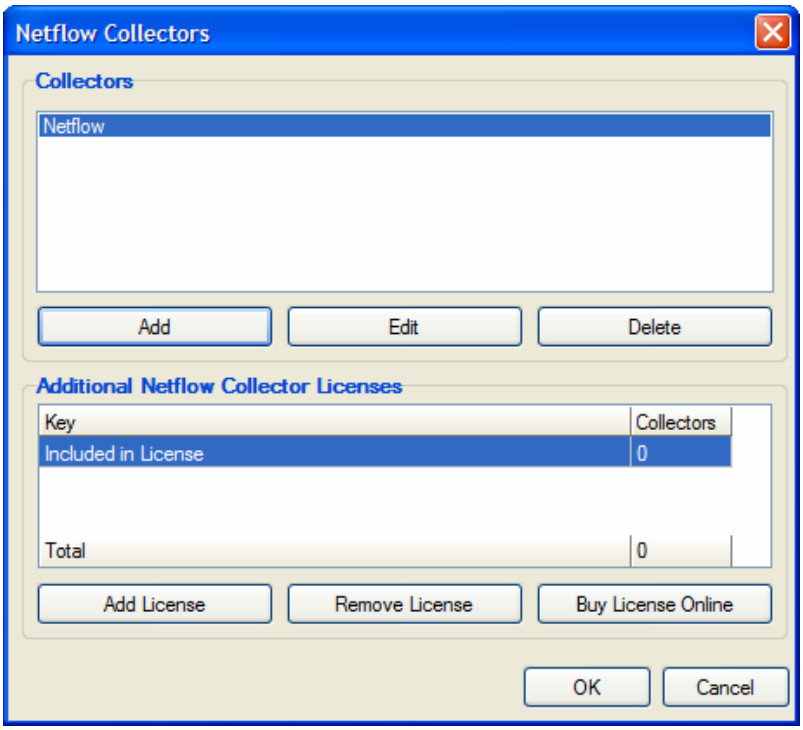
Please use the menu item **Extras|NetFlow Collectors** to set up licensing and Netflow Collectors.

Note 2: PRTG supports NetFlow version 5 only!

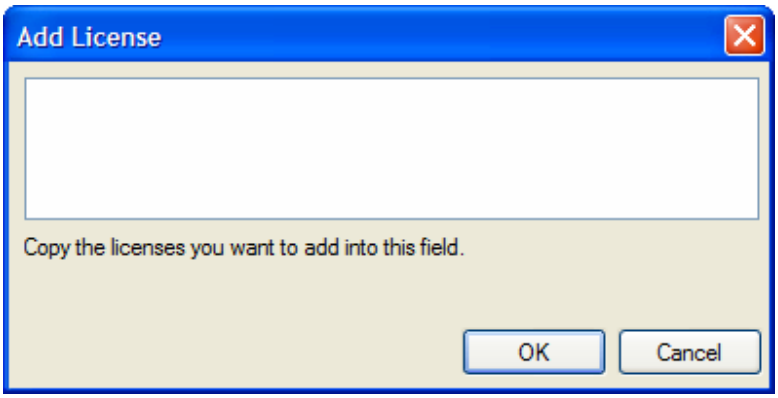
Setting up NetFlow Collectors

In order to use NetFlow monitoring you must set up a NetFlow Collector in PRTG. This instructs PRTG to accept NetFlow packets from the router coming in via a specific UDP port. The same IP and port must also be configured in the router configuration.

Using the menu item **Extras|Netflow Collectors** you can edit the setup for the collectors:

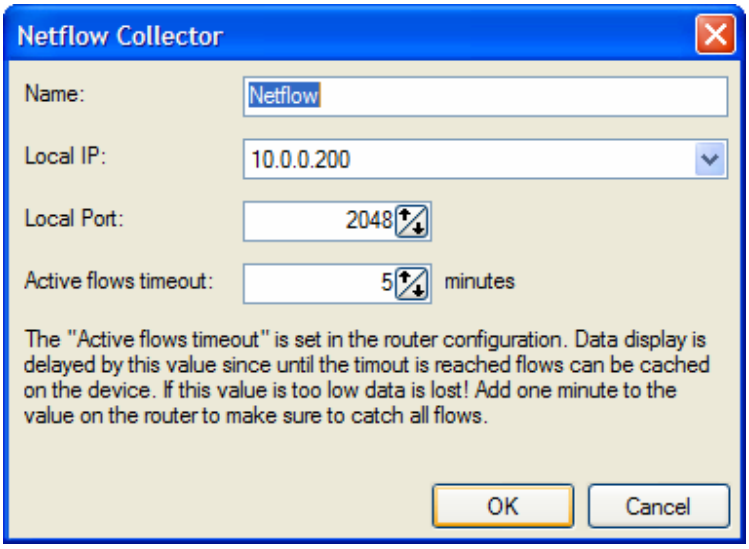


If you have purchased additional NetFlow Collector Licenses you can enable them by clicking on **Add License**:



Simply copy the license key(s) into the edit field and click OK. You should now see the corresponding number of NetFlow Collectors in the Licenses List.

Click on **Add** to create a new NetFlow Collector:


Netflow Collector
Name:
Netflow
Local IP:
10.0.0.200
Local Port:
2048
Active flows timeout:
5
minutes
The "Active flows timeout" is set in the router configuration. Data display is delayed by this value since until the timout is reached flows can be cached on the device. If this value is too low data is lost! Add one minute to the value on the router to make sure to catch all flows.
OK
Cancel

Here one can define the name of the collector, the local IP address, the local port, and the active flows timeout value.

Except for the name these settings must exactly match the configuration of your router. Please see the section "Configuration Tips for Cisco Routers and PRTG (NetFlow/SNMP)" for more information.

Have a special look at the last value (Active Flows Timeout). For non-high traffic situations (<10 MBit) a recommended value is 5 minutes, for higher traffic scenarios higher values of up to 30 minutes are recommended. This value has to be configured in the router!

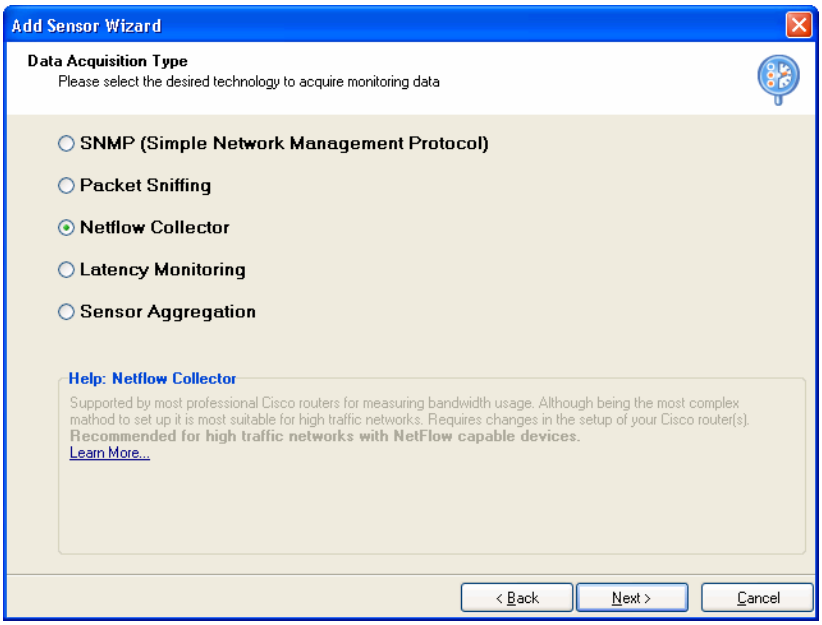
Starting the Add Sensor Wizard

In order to add a new sensor, click on the **Add Sensor** button in the sensor list's toolbar or select **Add New Sensor** from the **Edit** menu.

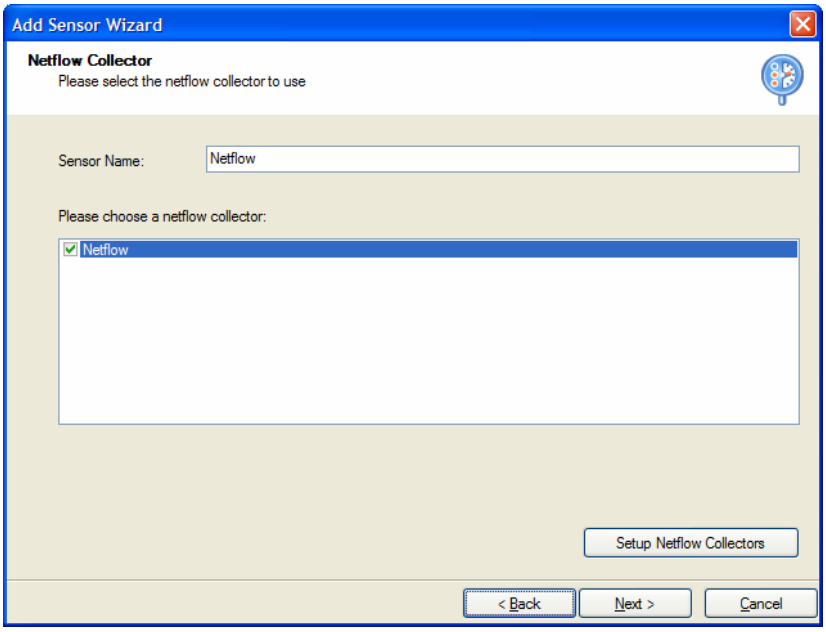
This will launch the **Add Sensor Wizard**.

Add Sensor Wizard
Welcome to the Add Sensor Wizard
This wizard will guide you step-by-step through the setup of new sensors for monitoring with PRTG Traffic Grapher.
Creating new sensors involves three main steps:
1. Selecting the data acquisition technology (SNMP, packet sniffing or NetFlow)
2. Selecting the device/server and scanning it for available sensors
3. Selecting the new sensors and choosing a group as well as an interval
Note: If you want PRTG Traffic Grapher to scan your network automatically for SNMP enabled devices please use the Automatic Network Discovery to create SNMP based sensors.
Please click "Next" to continue!
PAESSLER
< Back
Next >
Cancel

Click **Next** to proceed to the selection of the data acquisition.


Add Sensor Wizard
Data Acquisition Type
Please select the desired technology to acquire monitoring data
SNMP (Simple Network Management Protocol)
Packet Sniffing
Netflow Collector
Latency Monitoring
Sensor Aggregation
Help: Netflow Collector
Supported by most professional Cisco routers for measuring bandwidth usage. Although being the most complex method to set up it is most suitable for high traffic networks. Requires changes in the setup of your Cisco router(s).
Recommended for high traffic networks with NetFlow capable devices.
Learn More...
< Back
Next >
Cancel

Please select **NetFlow Collector**. This will lead to the NetFlow Collector selection screen:



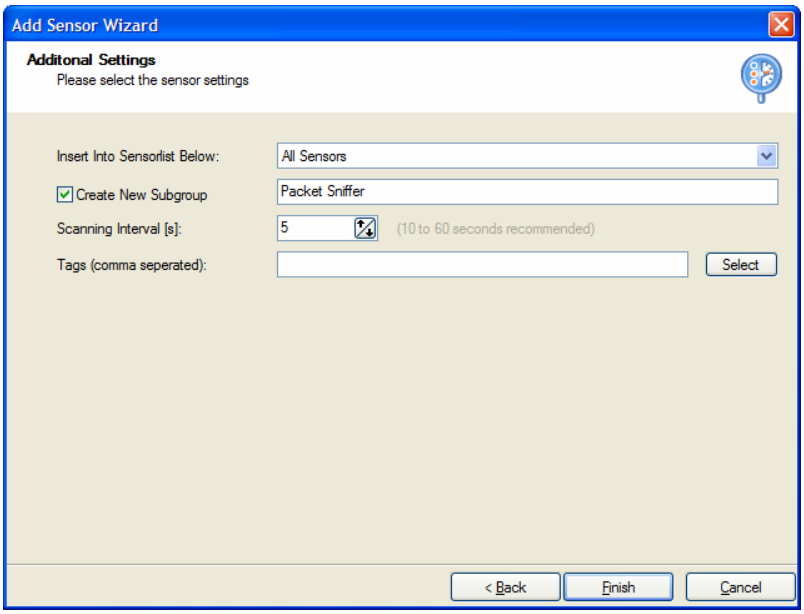
From the list, check the device(s) you would like to monitor. Then click the **Next** button. This will open the **Filter** window:

Filter and Protocol Setup

Please refer to the section Adding Packet Sniffer Sensors for detailed explanation of the filter and protocol setup.

Additional Settings

Once you have made your desired settings for the new SNMP sensor click on the **Next** button. This will bring up the **Additional Settings** window.



Choose a group of the sensor list that you want to add the new sensor(s) to. Optionally you can **Create a New Subgroup**.

Choose a group name that will help you to keep your sensors organized (e.g. "Firewall" or "LAN"). Also select the desired **scanning interval** in seconds. In most cases 30 seconds should be fine. Since NetFlow is a "push" technology, this value is only important for the screen update.

Finally you can add tags for the new sensors which will help you to categorize your sensors later. A tag consists of one or more words, e.g. switch, printer, 1st floor, 2nd floor, remote office, data center 1, data center 2, etc. Use commas to separate tags.

When you are finished selecting your options, click on **Finish**. This will finalize setting up the sensor and will start the monitoring of the sensor.

Adding Aggregation Sensors

Before you start

All the individual sensors must be properly set up before you can combine their readings into a new aggregation sensor (please see prior chapters on how to do this).

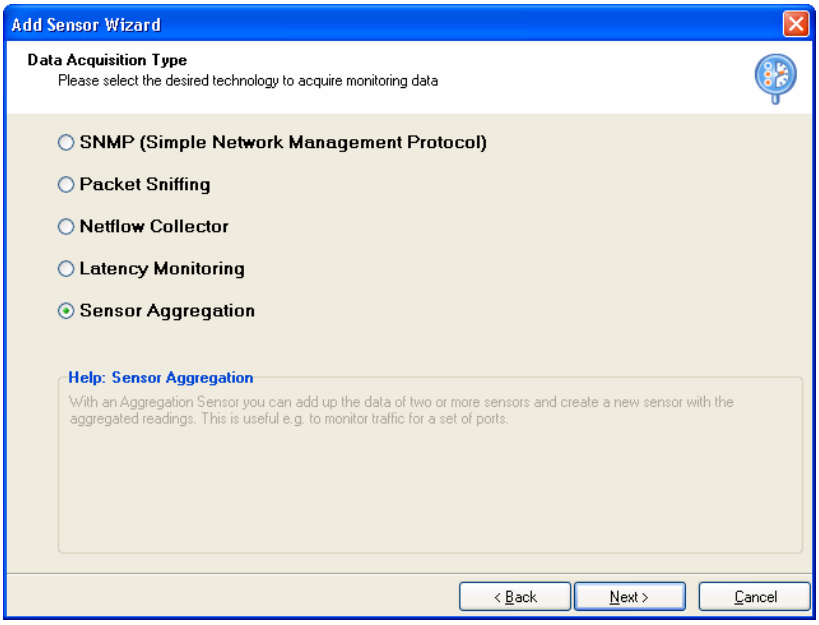
Starting the Add Sensor Wizard

In order to add aggregation sensors, click on the **Add Sensor** button in the sensor list's toolbar or select **Add New Sensor** from the **Edit** menu.

This will launch the **Add Sensor Wizard**.

Add Sensor Wizard
Welcome to the Add Sensor Wizard
This wizard will guide you step-by-step through the setup of new sensors for monitoring with PRTG Traffic Grapher.
Creating new sensors involves three main steps:
1. Selecting the data acquisition technology (SNMP, packet sniffing or NetFlow)
2. Selecting the device/server and scanning it for available sensors
3. Selecting the new sensors and choosing a group as well as an interval
Note: If you want PRTG Traffic Grapher to scan your network automatically for SNMP enabled devices please use the Automatic Network Discovery to create SNMP based sensors.
Please click "Next" to continue!
PAESSLER
< Back
Next >
Cancel

Click **Next** to proceed to the selection of the data acquisition.


Add Sensor Wizard
Data Acquisition Type
Please select the desired technology to acquire monitoring data
SNMP (Simple Network Management Protocol)
Packet Sniffing
Netflow Collector
Latency Monitoring
Sensor Aggregation
Help: Sensor Aggregation
With an Aggregation Sensor you can add up the data of two or more sensors and create a new sensor with the aggregated readings. This is useful e.g. to monitor traffic for a set of ports.
< Back
Next >
Cancel

Please select **Sensor Aggregation** and click **Next**. This will show the **Aggregation Sensor Selection** page

Enter a name for the sensor and then choose whether you want to work with delta sensors (e.g. traffic sensors) or gauge sensors (e.g. CPU loads).

PRTG then shows a list of available sensors and their channels. Now enable the checkboxes for the desired sensors and click N**ext** to finalize the sensor creation.

Working with Aggregation Sensors

As soon as you have created an Aggregation Sensor you can use it in PRTG's Web and Windows GUI just like any other sensor (with some minor exceptions, see below).

Double click the sensor in the sensor list to edit the sensor: Here you can add and remove channels from the aggregation. You can add additional channels with another set of sensors, too.

Notes and Limitations

There are some limitations for aggregation sensors:

- One aggregation sensor can only work with either delta or gauge sensors.
- All channels used for an Aggregation Sensor should use the same unit setting (otherwise the generic unit "#/unknown" will be used).
- Due to timing and rounding effects you may see small discrepancies when comparing aggregation sensors with their source channels.
- You can not re-use Aggregation Sensors to create another Aggregation Sensor (folding).
- There is no sum channel for the aggregated sensor.
- In the graphs the data lines for Aggregation Sensors appear slightly shifted to the right (=later) compared to the data lines of the source channels

because the aggregation sensor reads the data from the other sensors after they have aquired it, which creates a delay.

If delta sensors are used for aggregation:

- The scanning interval for the Aggregation Sensor must be at least three times the maximum scanning interval of the source sensors. The multiplier should always be an integer value (3 or higher).
- It is recommended that all source sensors should have the same scanning interval setting (e.g. 10 seconds sensor intervall and 30 seconds aggregation scanning, or 20 seconds & 60 seconds).
- Aggregated delta sensors ignore overflow values (see High Compatibility Mode).

If gauge sensors are used for aggregation:

- The scanning interval for the Aggregation Sensor should be the same as the scanning interval of all source sensors.
- It is recommended that all source sensors should have the same scanning interval setting.

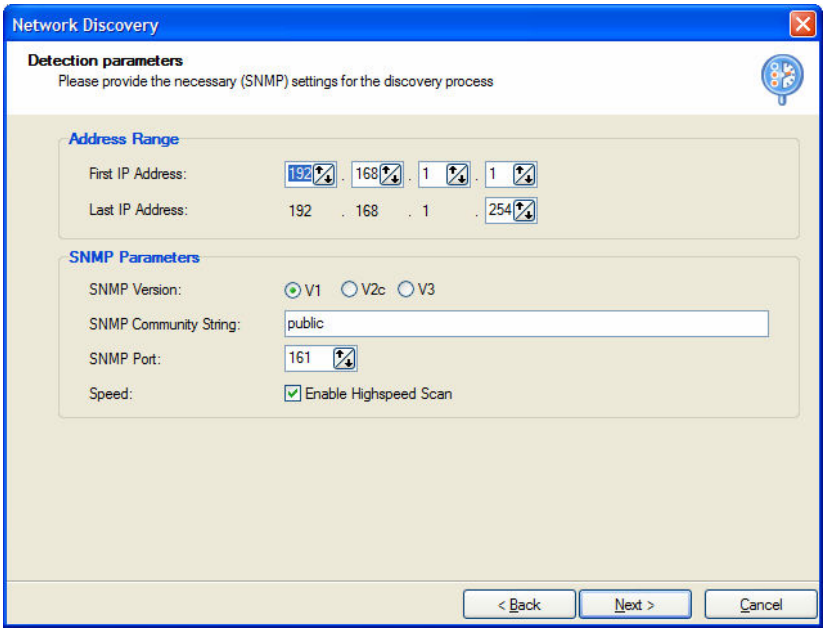
Automatic Network Discovery

For SNMP based networks PRTG Traffic Grapher offers the option to scan your network for available SNMP devices and to automatically create SNMP based sensors for all devices found.

To start this process select **Automatic Network Discovery** from the **Extras** menu.

Network Discovery
Welcome to the Network Discovery Wizard
This wizard will guide you through the automatic discovery of SNMP devices/interfaces and creation of corresponding SNMP sensors.
The Automatic Network Discovery involves three main steps:
1. First you must choose an IP address range you want to scan
2. Then PRTG scans your network for SNMP enabled devices, which can take a few minutes
3. Afterwards you can choose the new sensors from a list of all discovered SNMP items.
Please click "Next" to continue!
PAESSLER
< Back
Next >
Cancel

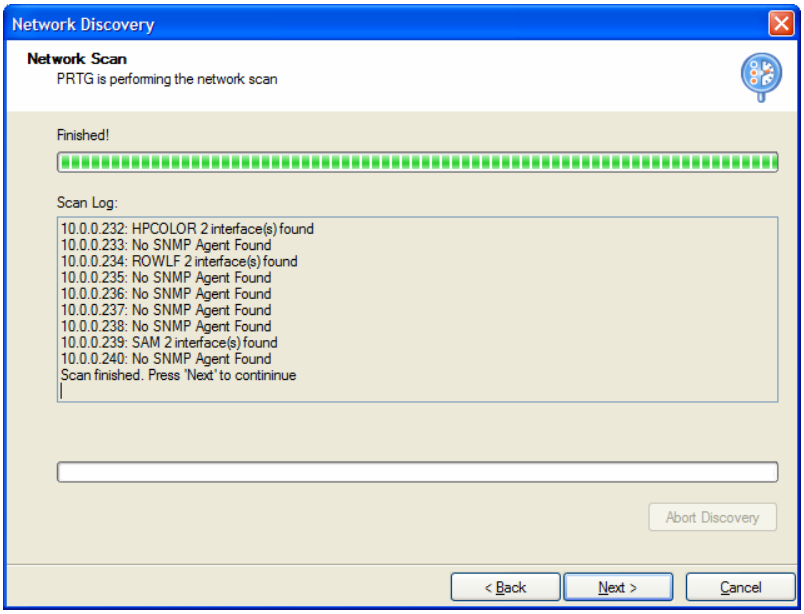
Click on **Next** to select the IP range:



Select the **First IP Address** and **Last IP Address** to scan for the test and – if you do not use the default values – edit the SNMP settings **Community String** and **Port**.

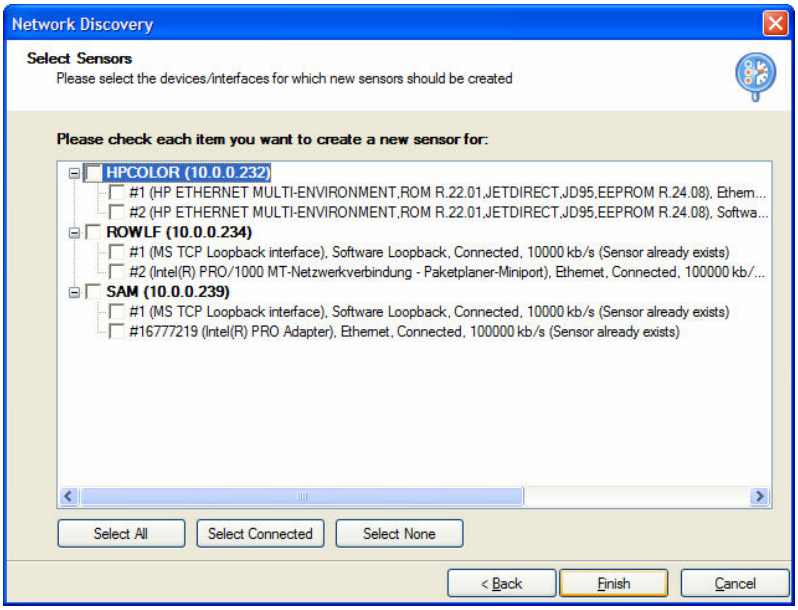
The **Enable Highspeed Scan** setting should be fine for most networks. If PRTG fails to discover one or more devices when scanning your network try to disable this setting (scanning will take about 5-10 times longer).

As soon as you click **Next** the scan is started, it will take about 3-10 seconds per IP address:



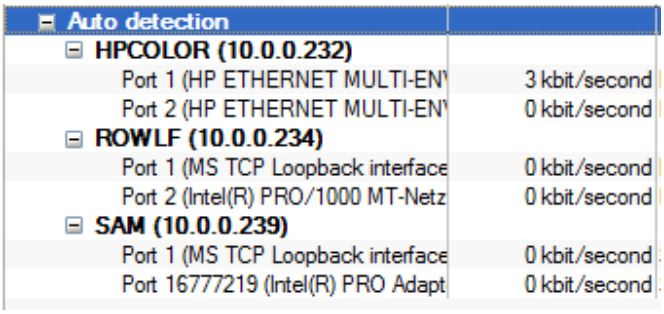
You can see the progress in the scan log. After the scan has finished click **Next** and you will get a list of devices and possible sensors found in your network.

Note that ports which are not connected and sensors that are already configured in PRTG will not be checked by default, so you can run the discovery process multiple times without creating new sensor twice.


Network Discovery
Select Sensors
Please select the devices/interfaces for which new sensors should be created
Please check each item you want to create a new sensor for:
HPCOLOR (10.0.0.232)
#1 (HP ETHERNET MULTI-ENVIRONMENT,ROM R.22.01,JETDIRECT,JD95,EEPROM R.24.08), Ethem...
#2 (HP ETHERNET MULTI-ENVIRONMENT,ROM R.22.01,JETDIRECT,JD95,EEPROM R.24.08), Softwa...
ROWLF (10.0.0.234)
#1 (MS TCP Loopback interface), Software Loopback, Connected, 10000 kb/s (Sensor already exists)
#2 (Intel(R) PRO/1000 MT-Netzwerkverbindung - Paketplaner-Miniport), Ethernet, Connected, 100000 kb/...
SAM (10.0.0.239)
#1 (MS TCP Loopback interface), Software Loopback, Connected, 10000 kb/s (Sensor already exists)
#16777219 (Intel(R) PRO Adapter), Ethernet, Connected, 100000 kb/s (Sensor already exists)
Select All
Select Connected
Select None
< Back
Finish
Cancel

Choose the sensors you want to create by checking/unchecking the check boxes and click on **Finish**.

In the sensor list you will find a new top-level group with the title **Auto Detection** (at the bottom of the list) with one sub-group for each device that contains all the sensors for this device:



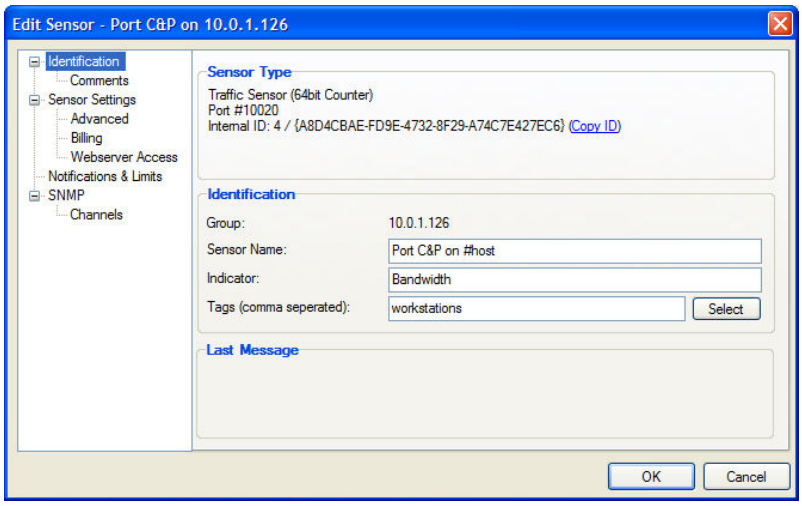
Editing Sensors

You can edit a sensor by double clicking its entry in the sensor list. There are a number of settings that apply to all sensor types, as well as individual settings for each sensor type.

The settings are arranged on a number of pages and you can select the desired entry on the left hand side.

Identification Settings

This page covers the basic data about the sensor:

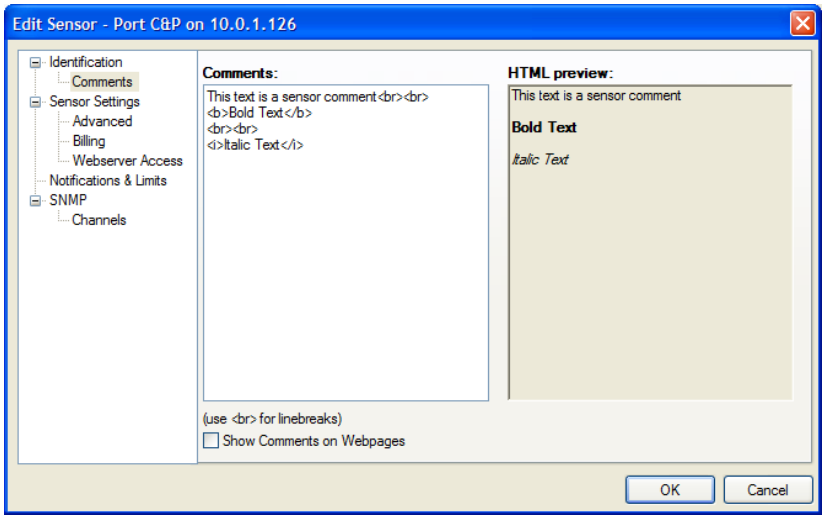


The **sensor type** is defined during the initial sensor setup and can not be edited (except the OID for library and custom sensors).

In the **Identification** section of this window, you can define the **Sensor Name**, which will be used to identify the sensor. You can also enter a value for the **Indicator** field as well as tags.

Comments Settings

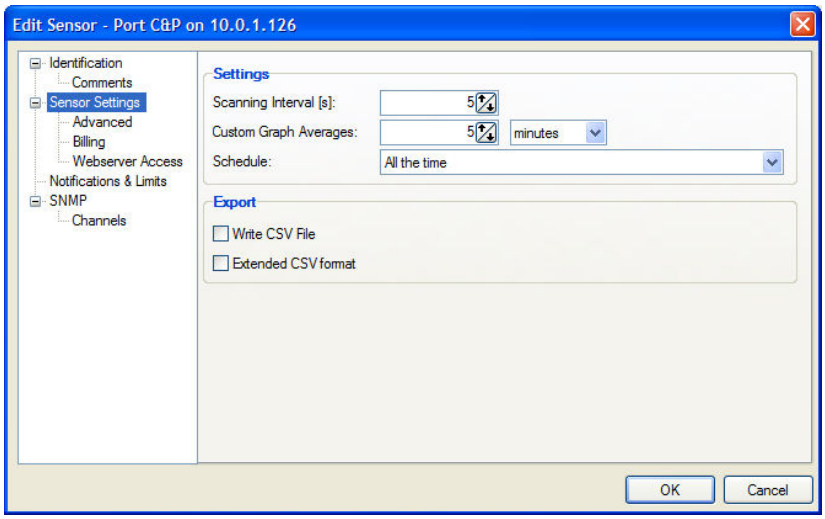
On this tab you can enter any comments regarding this sensor. Use simple HTML for highlighting, e.g. <b> for bold, <br> for a new line, etc. You will see a preview of the rendered HTML on the right.



By enabling the **Show Comments on Webpages** checkbox you can also make this comment visible in the web interface.

Sensor Settings

In the **Settings** section, you can define the **scanning interval** (in seconds) – this interval defines at what rate the device is scanned for information.



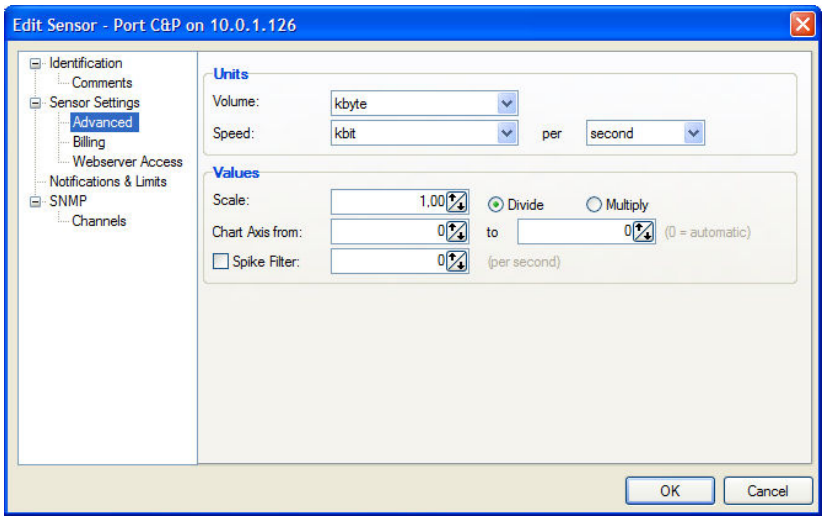
The **Custom Graph Averages** is used to determine the average value used for the custom graph type. You can enter a value and then define the time span according to seconds, minutes, hours, or days.

If you do not want to monitor the sensor all the time you can select a **schedule** from the list. See the section Schedules Settings for more information.

To export the raw monitoring data into files, checking the **Write CSV File** checkbox will enable the generation of one CSV file per sensor per day. **Extended CSV format** dumps even more data into the CSV file. These CSV files will then contain the results of each single request and can be used to import the data into other programs for further analysis. See the section "What do the values in the exported CSV log file say?" for more information.

Advanced Settings

In the **Units** settings, you can define what units to use for the volume, as well as for the speed.



Please select the units from the drop-down menu. These units will affect the web view, as well as the reports generated for this particular sensor.

In the **Values** settings you can define the **Scale** – the raw result of the sensor is either divided or multiplied by this value (select the appropriate radio button).

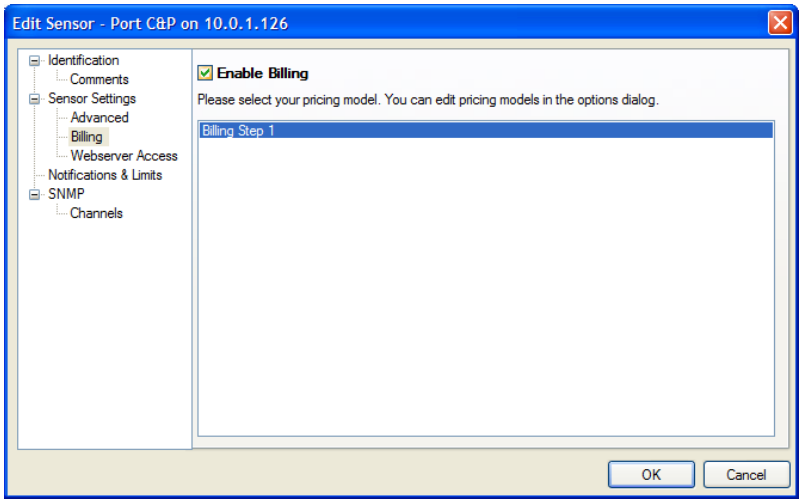
In the **Chart Axis from/to fields** you can define a value to be used for the range of the vertical axis of the graph. The standard value of "0" scales the vertical axis automatically.

If you want to filter spikes, check the **Spike Filter** checkbox and enter a maximal value (per second) in the right field. This will avoid the graphs spiking when erroneous values are reached.

Note: Spike filter values must be entered with the default values of the sensor. The **Units** fields do not affect this setting!

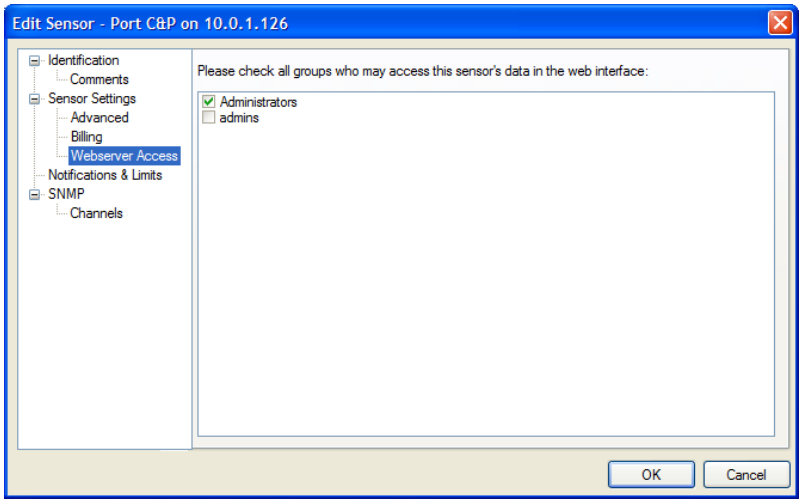
Billing Settings

If you want to use PRTG's billing system you must first setup pricing models in the **Extras|Options** dialog. Then you can select the correct pricing model for this sensor here. See the Billing section for more details.



Access Settings

On this tab you can specify what user groups may access this sensor's data in the web interface. Users and groups are managed in the **Extras|Options** dialog.



Notifications & Limits Settings

PRTG can send out notifications if an error is discovered by a sensor or a defined threshold and volume has been reached.

There are three types of notifications available in PRTG Traffic Grapher:

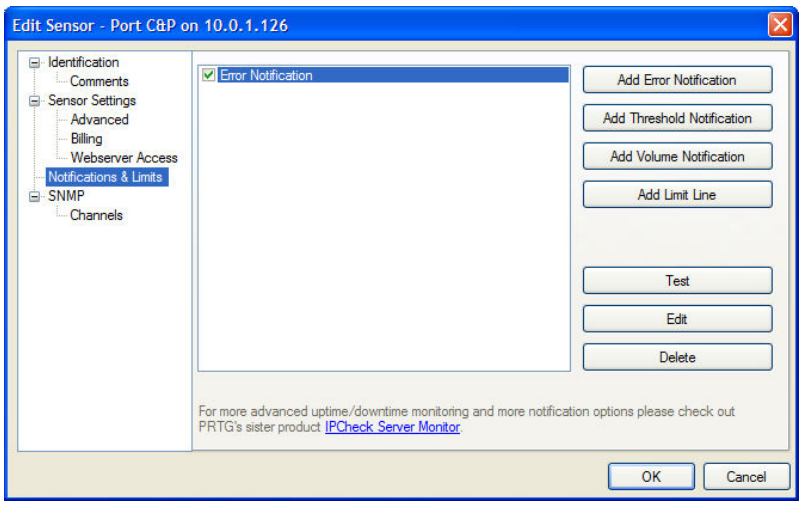
- Error Notifications
- Threshold Notifications
- Volume Notifications

Each sensor can have an unlimited number of notifications. Each notification can

- Send an email
- Send an http request

- Execute an EXE or batch file
- Change the sensor's chart background

Additionally you can define horizontal limit lines **(Add Limit Line)** that are shown in the graphs.



Using the **Add…** buttons you can add new notifications and limit lines (see below).

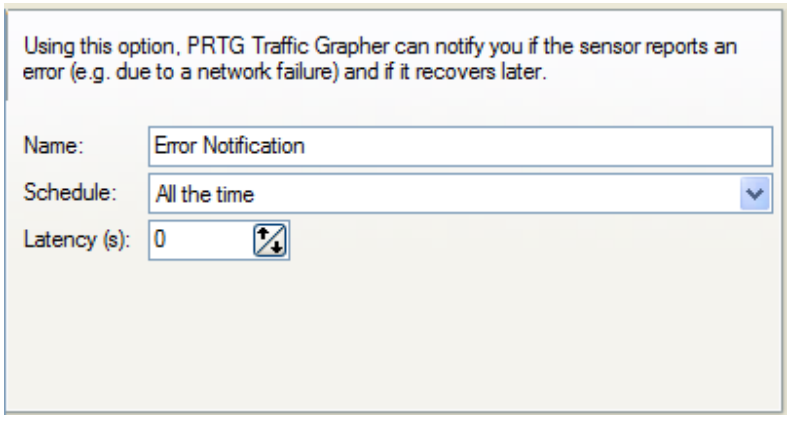
Clicking the **Edit** button will open up the notifications dialog and allow you to edit its settings. The **Delete** button will delete the notification entirely.

Click the **Test** button to send a test notification.

In order to select / deselect a notification, simply click on the checkbox in front of it to enable or disable the notification.

Error Notifications

Using the **Add Error Notification** button, you can set up notifications that will be triggered as soon as an error is encountered for a sensor.

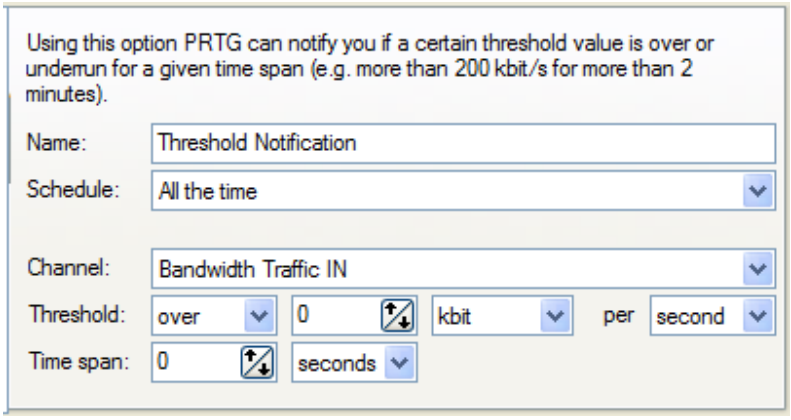

Using this option, PRTG Traffic Grapher can notify you if the sensor reports an error (e.g. due to a network failure) and if it recovers later.
Name:
Error Notification
Schedule:
All the time
Latency (s):
0

PRTG will optionally wait for the number of seconds you set in the **latency** setting before sending out the notification in order to give the device a chance to recover.

If you do not want to be notified at all times you can select a **schedule** from the list. See the section Schedules Settings for more information.

Threshold Notifications

Using the **Add Threshold Notification**, it is possible to add a notification which will alert when a sensor has reached a certain threshold value.



If you do not want to be notified at all times you can select a **schedule** from the list. See the section Schedules Settings for more information.

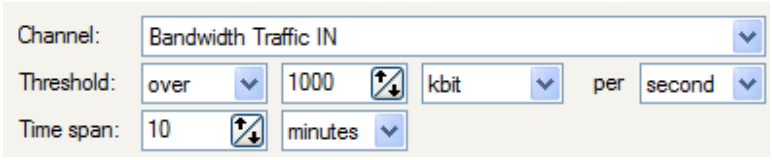
The **Channel** setting allows you to select from the IN, OUT, or the SUM of both, in order to base the threshold calculation on this value.

Under the **Threshold** entry, you will find four drop-downs. These allow you to set whether the threshold is to be defined over or under a specific value. This value is defined in units per time, as set by the last drop-downs.

The third row allows you to define the time span for which these measurements are to be considered.

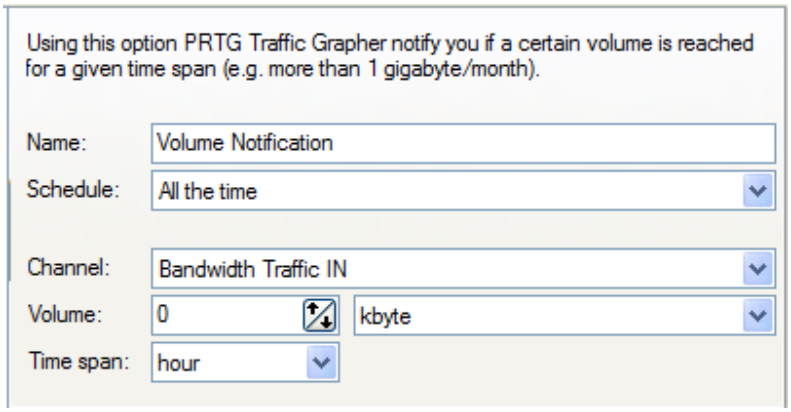
Note: Make sure that the time span used is greater than the polling interval set for this sensor!

As such, if you want a threshold notification to be sent when the inbound bandwidth reading goes over 1000 kbit/second for a time span of more than 10 minutes, the settings would look like this:



Volume Notifications

Using the **Add Volume Notification**, it is possible to add a notification which will alert whenever a sensor has reached a certain volume.

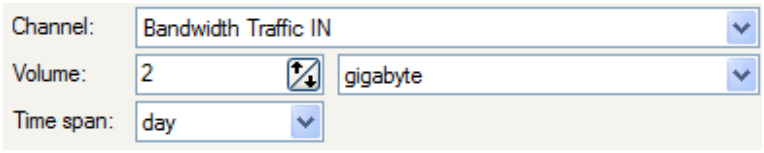


If you do not want to be notified at all times you can select a **schedule** from the list. See the section Schedules Settings for more information.

The **Channel** option will allow you to select the desired channel for the sensor from the drop-down menu.

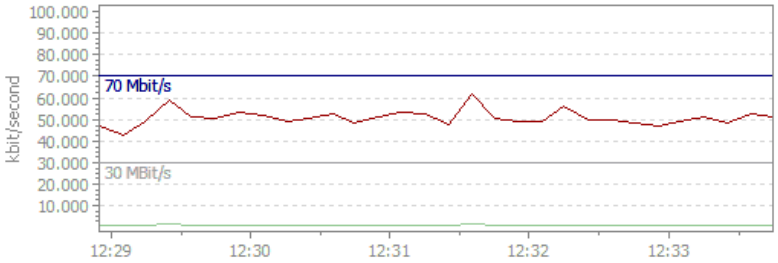
In the **Volume** fields, enter the amount, as well as the unit for which the notification is to be sent, once this volume has accumulated.

In the time span field, define for which time span this volume notification shall be sent. Basically, you can set up a sensor so as to send out a notification if, for example, a sensor reaches 2 Gigabyte in a day. This setup would look like this:



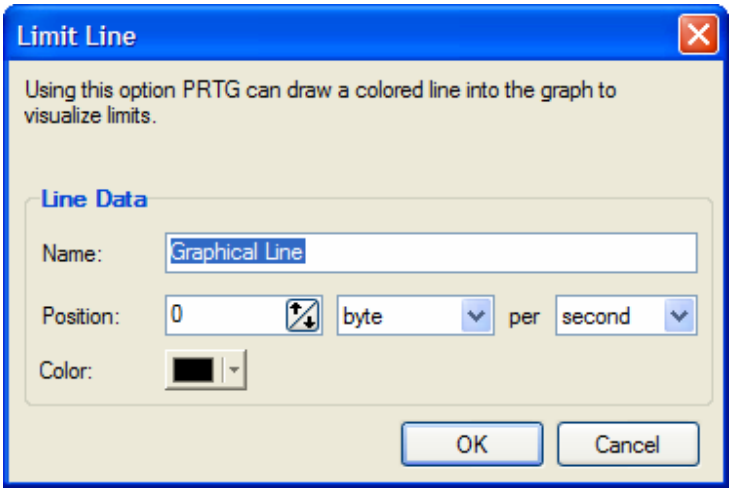
Limit Lines

To make it easier to judge the load of a data line (or any other measured value) it is a good idea to add horizontal lines to the graph which e.g. show the maximum speed of the data line. Such a graph looks like this:



We have added a gray line for 30 MBit/s and a blue line for 70 MBit/s to this chart and have additionally set the sensor's maximum vertical axis to 100 Mbit/s.

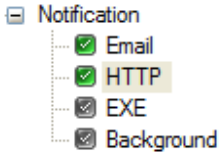
Click on **Add Limit Line** to add such a line:



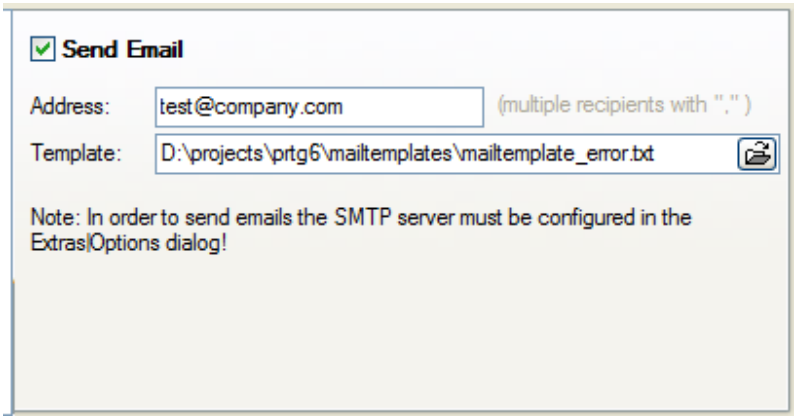
Please choose a **name**, **position** and **color** and click **OK**.

Common Settings for Notifications

For all notification types you have the option to send an email, send a HTTP request to a web server, or to run an external program or batch file.



The first notification option is **Email**: An email is sent to an address that you specify using an SMTP server. (Note: The configuration for the SMTP server is done under the Extras|Options dialog.)



This option can be enabled by the **Send Email** checkbox.

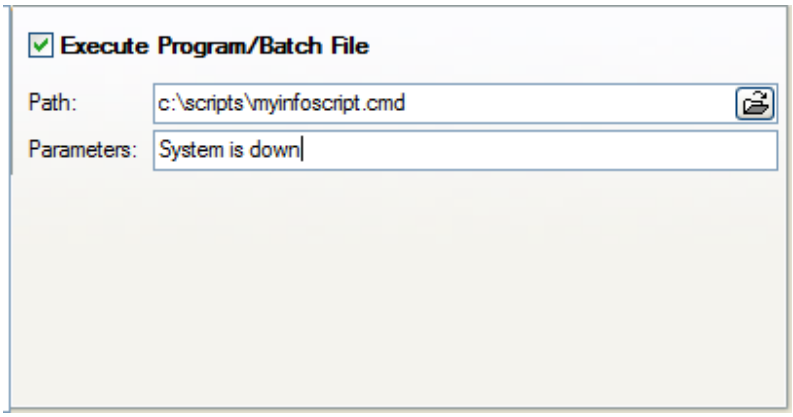
Please provide the **e-mail address** to send the email to. If you want the email to go to multiple addresses please separate these addresses with a comma ",".

The second field allows one to select a mail **template** file to be used for this notification. The first line of the template file is used as the email topic. You can use placeholders (see below) inside the template file. If there is an .htm-file with the same filename PRTG will use both files to create a combined text and HTML mail.

The second notification option is **HTTP**: An http GET request is sent by PRTG:

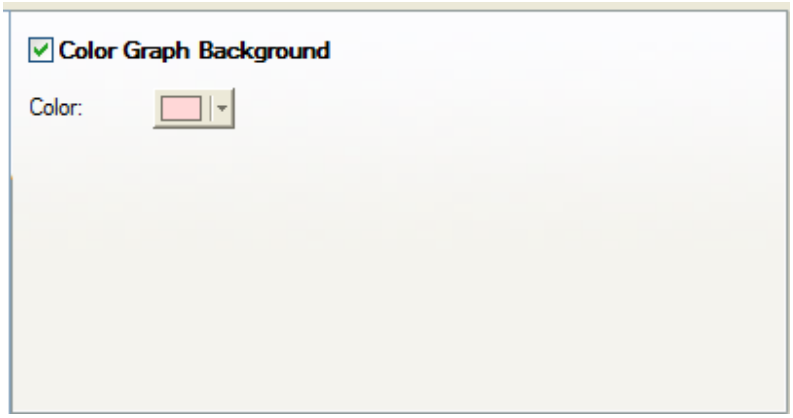
Please enter a HTTP GET URL and PRTG will – in case the notification is fired – send an HTTP request to this URL. Placeholders (see below) can be used in the URL.

The third notification option is **EXE**: An EXE file or a batch file is executed by PRTG:



Please provide the path to the EXE file or BAT/CMD file as well as the parameters. Placeholders (see below) can be used in the parameters field.

The fourth notification option is **Background**: You can choose a color that will be used as the chart background whenever the notification is triggered. This way a chart with a failing sensor can easily be identified on the screen.



For the email template, the HTTP URL, and the execute parameters you can use the following placeholders:

#group	Name of the sensor's group
#sensor	Name of the sensor
#message	The message of the notification
#info	The state of the sensor (UP, DOWN, etc.)
#error	Detailed error message
#date	Current date
#time	Current time

Here is a sample for a mail template using placeholders:

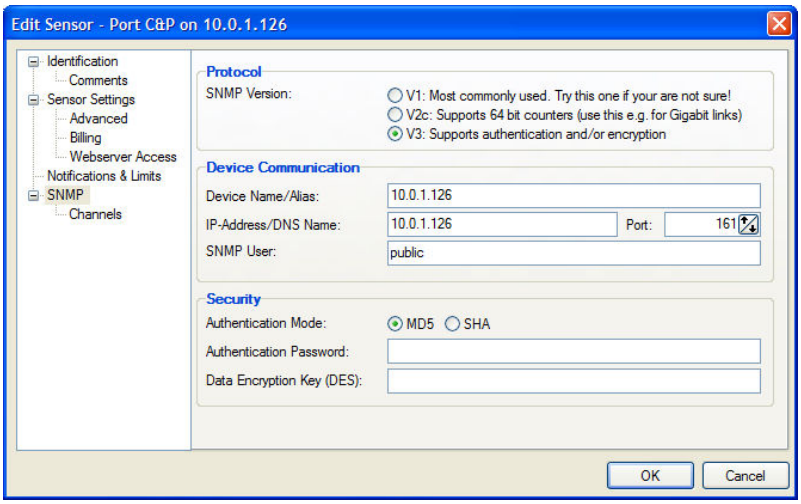
```
[PRTG] Notification: #info, #sensor
Date: #date #time
Group: #group
Sensor: #sensor

#message
```

Communication Settings

In this tab you can control the communication of the sensor. Depending on the sensor type there are different settings:

Communication Settings for SNMP Sensors



In the **Protocol** section you can choose between SNMP Version 1, 2c and 3.

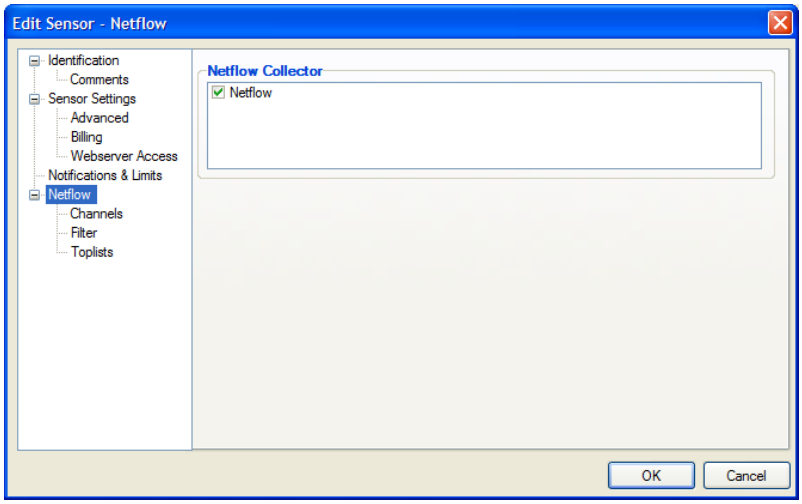
Under the **Device Communication** settings, you can define a **Device Name / Alias** for the sensor. In the field **IP-Address** you can configure the device's IP address, as well as enter the appropriate **Port** number for the SNMP communication.

For SNMP V1 and V2c you can set the **community string**. The default value of this field is "public".

For SNMP V3 you must set the **security** settings, **Authentication Mode** and **Password**.

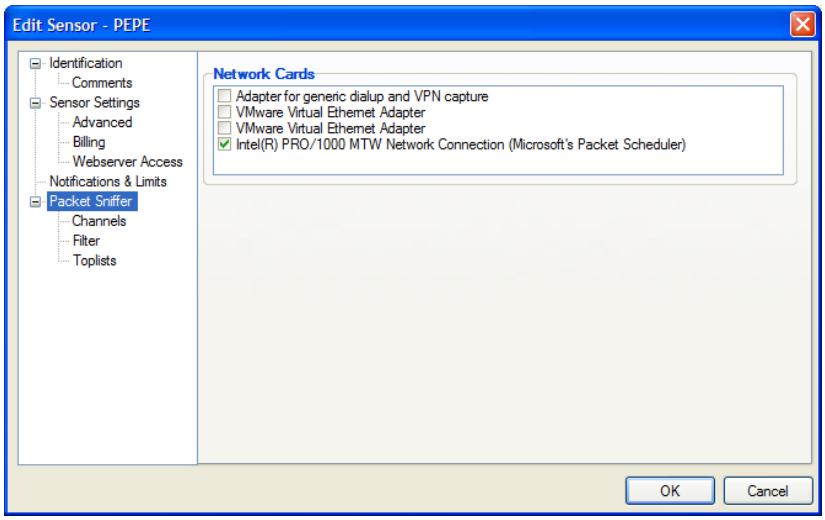
To enable encryption please enter a **Data Encryption Key**. Leave the field empty to disable encryption.

Communication Settings for Netflow Sensors



Please choose the Network Collector the current sensor shall work with, you can choose one or more collectors. Note: Netflow Collectors are set up in the **Extras** menu.

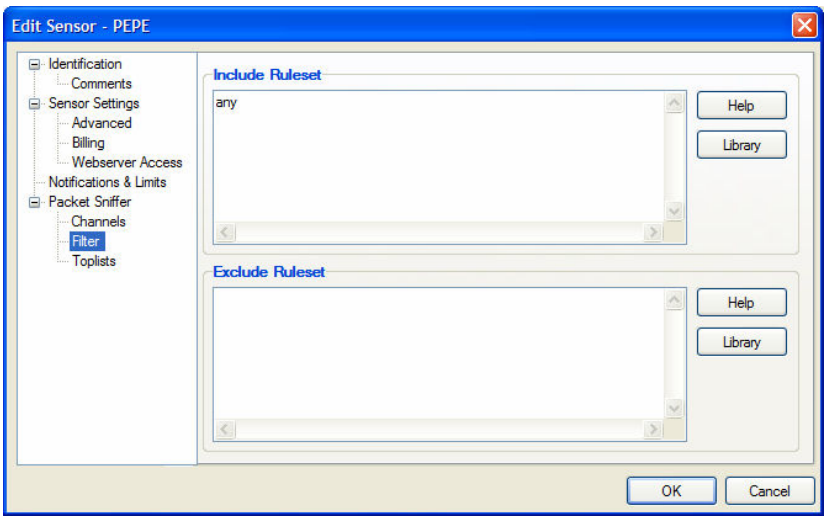
Communication Settings for Packet Sniffer Sensors



Here you can choose what network card(s) this sensor is monitoring, you can choose one or more cards.

Filter Settings

For Packet Sniffer and NetFlow sensors you can edit the rule sets of the filter here:

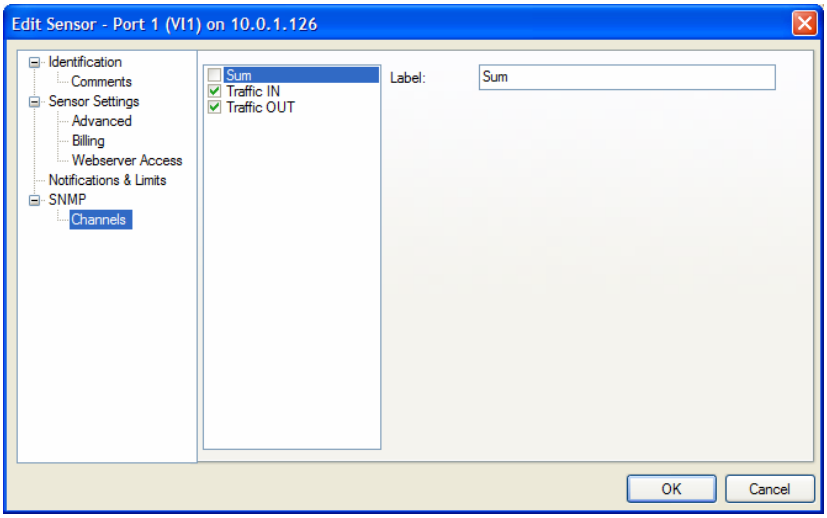


See the section Filter Setup for details.

Channel Settings

Depending on the sensor type the **Channels** tab allows you to select what data of a sensor is shown in graphs and tables.

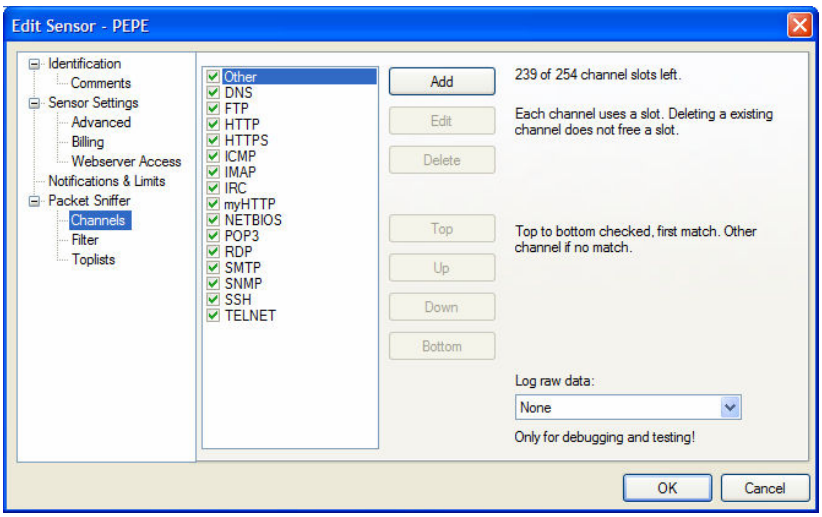
For SNMP Traffic Sensors there are three channels:



Use the checkboxes to enable and disable a channel. Using the edit box on the right you can change a channel's name.

For other SNMP sensor types the channels can not be edited.

For NetFlow and Packet Sniffer sensors you can edit and enable/disable the protocol channels:



Use the checkboxes to enable and disable the display of a channel (data is still collected). Use the buttons to add, edit, or delete channels. Or sort them using the arrow buttons to the right.

See the section Protocol Setup for more details.

Log raw data (on the bottom right) captures data in a file in the CSV format. Bear in mind that this captures one entry per packet and, as such, the csv file grows very large. This is mainly to help in setting up and debugging configurations. Note: this file is stored in the folder **c:\documents and settings\all users\prtg traffic grapher**.

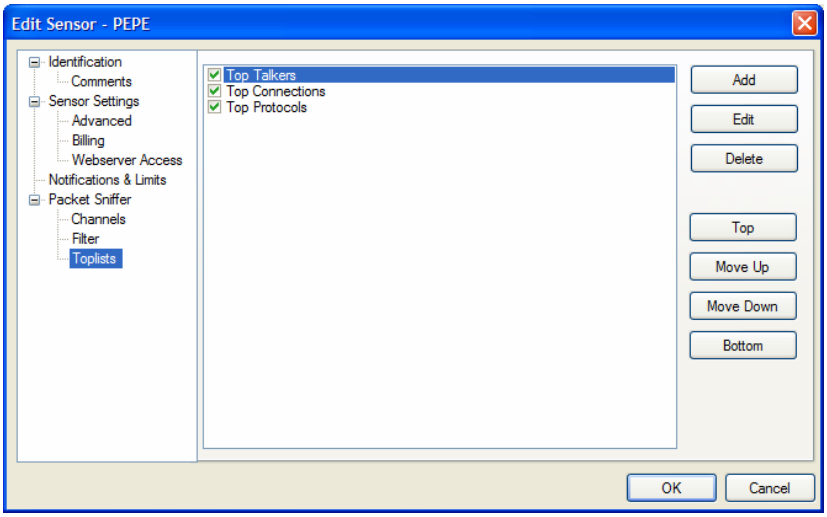
Note: You can only define 255 channels for one sensor. Deleting older channels from the channel list will NOT increase the amount of remaining slots available, because in the historic data the old channels still require their previously allotted slots.

Toplists Settings

Note 1: When working with Toplists be aware that privacy issues can come up for certain configurations of this feature. Using Toplists you can track all single connections of an individual PC to the outside world and you, as the administrator, must make sure that it is legal for you to configure PRTG like this.

Note 2: Keep in mind that Toplists are also shown in the web interface. You may not want to show lists of domains used in your network to others. In this case protect your PRTG webserver using passwords.

For Packet Sniffer and NetFlow sensors you can enable and edit one or more Toplists here:



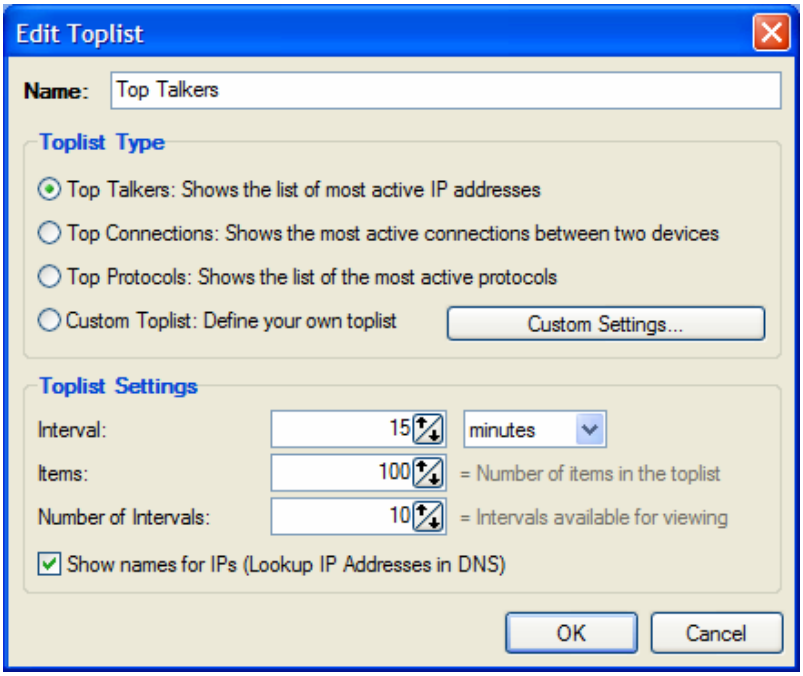
When you set up a new NetFlow or Packet Sniffer sensor three Toplists are created automatically:

- Top Talkers
- Top Connections
- Top Protocols

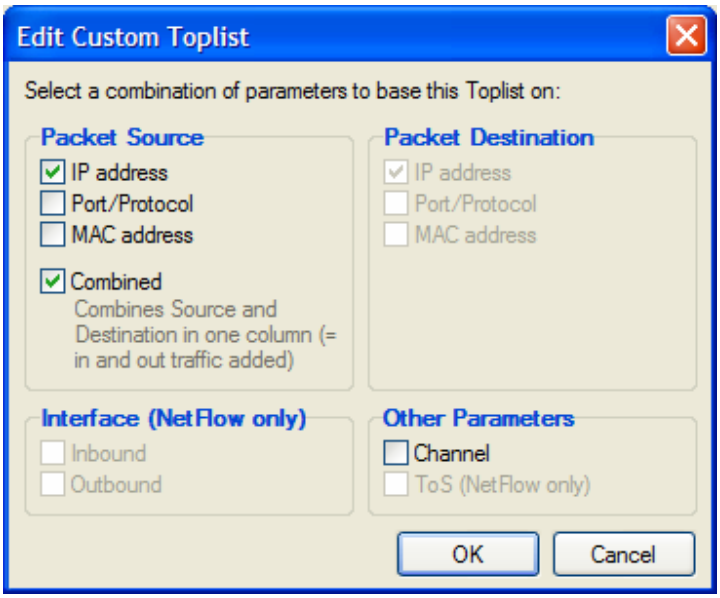
This covers the most basic needs, but you can also edit the three toplists or create additional ones. Use the **Add**, **Edit** and **Delete** buttons to manage your Toplists.

Editing a Toplist

Click on Edit to change the settings of a Toplist:



First you need to select a **Toplist Type**: Choose from the three standard types or choose **Custom Toplist** to define your own Toplist parameters using the **Custom Settings** Button:



Depending on the Sensor type you have various parameters at your disposal that you can use to build your Toplist. After choosing your desired combination click **OK** to return to the Toplist dialog.

In the Toplist Settings group you can specify

- **Interval**: How long should data for a Toplist be gathered before a new Toplist is started
- **Items**: How many items do you want to see in your Toplist
- **Number of Intervals**: How many recent Toplists should PRTG keep in memory for access by the user

Finally you have the option to have PRTG resolve all IP addresses that it comes across using reverse DNS requests.

Working with Custom Graphs

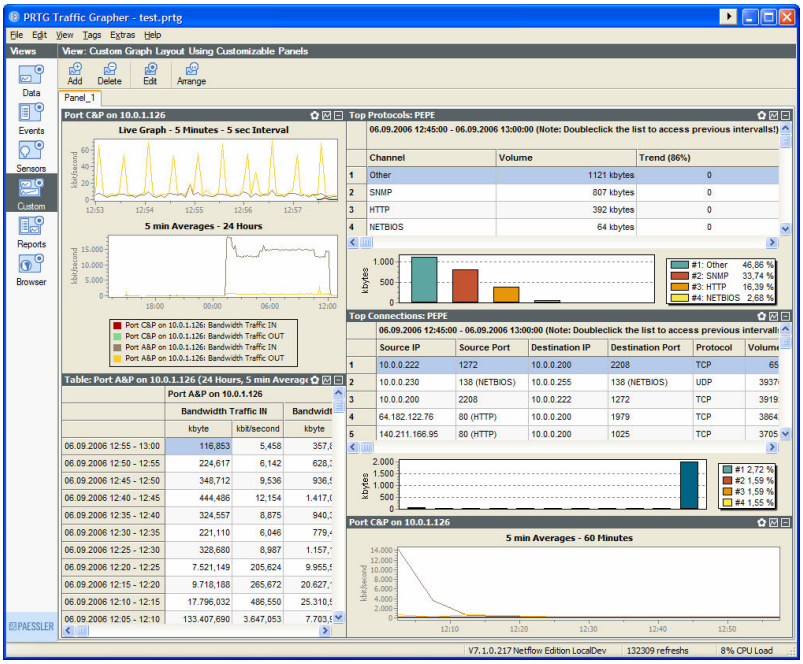
In the Data View you have fast access to graphs and you can specify any combination of sensors to show in one graph by selecting several items from the sensor list using your mouse – But: you can not change the layout and look & feel of the data individually for each sensor nor can you arrange your own layout of graphs and tables.

This is what “Custom Panels” are used for.

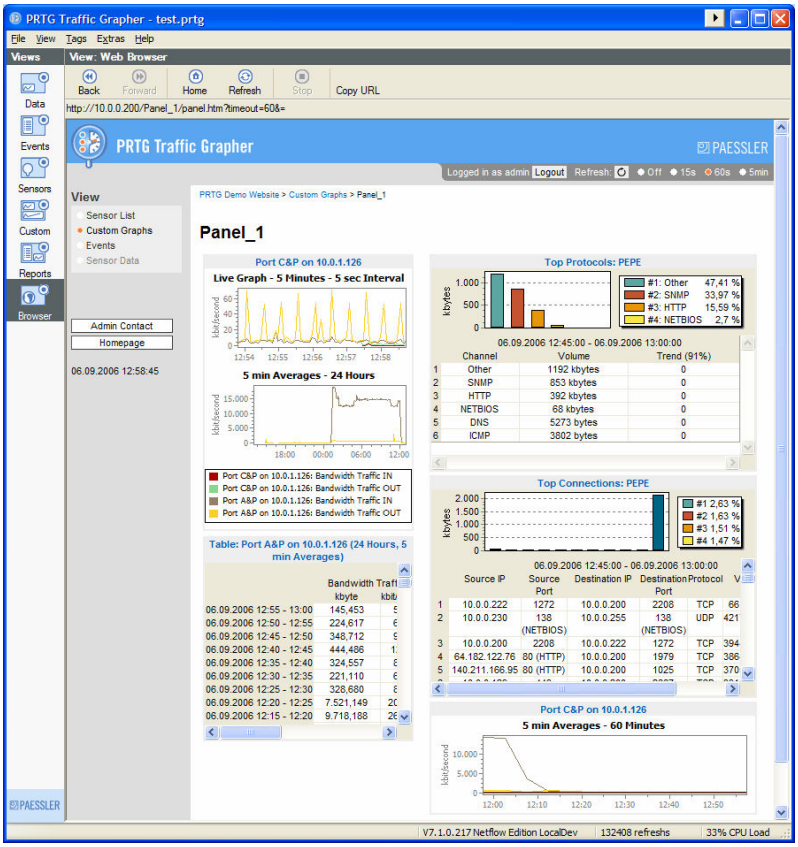
The Concept of Custom Panels

For each panel you can specify the the layout of the grid and the content of each grid section. And you can combine graphs and tables. Finally, panels can be viewed from the web interface with the same layout and you can give each panel different access policies for users accessing the Web interface.

This screenshot shows a panel with graphs and tables:


PRTG Traffic Grapher - test.prtg
File Edit View Tags Extras Help
Views
View: Custom Graph Layout Using Customizable Panels
Add Delete Edit Arrange
Data
Events
Sensors
Custom
Reports
Browser
Panel_1
Port C&P on 10.0.1.126
Live Graph - 5 Minutes - 5 sec Interval
5 min Averages - 24 Hours
Port C&P on 10.0.1.126: Bandwidth Traffic IN
Port C&P on 10.0.1.126: Bandwidth Traffic OUT
Port A&P on 10.0.1.126: Bandwidth Traffic IN
Port A&P on 10.0.1.126: Bandwidth Traffic OUT
Top Protocols: PEPE
06.09.2006 12:45:00 - 06.09.2006 13:00:00 (Note: Doubleclick the list to access previous intervalls!)
Channel Volume Trend (86%)
1 Other 1121 kbytes 0
2 SNMP 807 kbytes 0
3 HTTP 392 kbytes 0
4 NETBIOS 64 kbytes 0
#1: Other 46,86 %
#2: SNMP 33,74 %
#3: HTTP 16,39 %
#4: NETBIOS 2,68 %
Top Connections: PEPE
06.09.2006 12:45:00 - 06.09.2006 13:00:00 (Note: Doubleclick the list to access previous intervalls!)
Source IP Source Port Destination IP Destination Port Protocol
1 10.0.0.222 1272 10.0.0.200 2208 TCP
2 10.0.0.230 138 (NETBIOS) 10.0.0.255 138 (NETBIOS) UDP
3 10.0.0.200 2208 10.0.0.222 1272 TCP
4 64.182.122.76 80 (HTTP) 10.0.0.200 1979 TCP
5 140.211.166.95 80 (HTTP) 10.0.0.200 1025 TCP
#1 2,72 %
#2 1,59 %
#3 1,59 %
#4 1,55 %
Table: Port A&P on 10.0.1.126 (24 Hours, 5 min Average
Port A&P on 10.0.1.126
Bandwidth Traffic IN
kbyte kbit/second
06.09.2006 12:55 - 13:00 116,853 5,458
06.09.2006 12:50 - 12:55 224,617 6,142
06.09.2006 12:45 - 12:50 348,712 9,536
06.09.2006 12:40 - 12:45 444,486 12,154
06.09.2006 12:35 - 12:40 324,557 8,875
06.09.2006 12:30 - 12:35 221,110 6,046
06.09.2006 12:25 - 12:30 328,680 8,987
06.09.2006 12:20 - 12:25 7.521,149 205,624
06.09.2006 12:15 - 12:20 9.718,188 265,672
06.09.2006 12:10 - 12:15 17.796,032 486,550
06.09.2006 12:05 - 12:10 133.407,690 3.647,053
Port C&P on 10.0.1.126
5 min Averages - 60 Minutes
PAESSLER
V7.1.0.217 Netflow Edition LocalDev
132309 refreshs
8% CPU Load

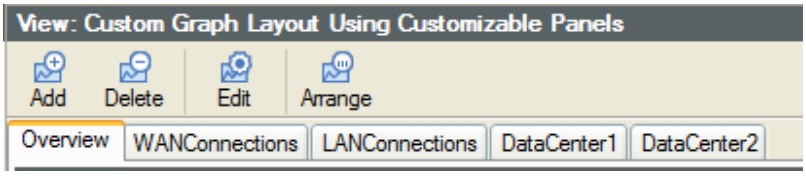
This second screenshot shows the same panel in the Web interface – it shows the same layout and data:


PRTG Traffic Grapher - test.prtg
File View Tags Extras Help
Views
View: Web Browser
Back Forward Home Refresh Stop Copy URL
http://10.0.0.200/Panel_1/panel.htm?timeout=60&=
PRTG Traffic Grapher
PAESSLER
Logged in as admin Logout Refresh: Off 15s 60s 5min
Data
Events
Sensors
Custom
Reports
Browser
View
Sensor List
Custom Graphs
Events
Sensor Data
Admin Contact
Homepage
06.09.2006 12:58:45
PRTG Demo Website > Custom Graphs > Panel_1
Panel_1
Port C&P on 10.0.1.126
Live Graph - 5 Minutes - 5 sec Interval
5 min Averages - 24 Hours
Port C&P on 10.0.1.126: Bandwidth Traffic IN
Port C&P on 10.0.1.126: Bandwidth Traffic OUT
Port A&P on 10.0.1.126: Bandwidth Traffic IN
Port A&P on 10.0.1.126: Bandwidth Traffic OUT
Table: Port A&P on 10.0.1.126 (24 Hours, 5 min Averages)
Top Protocols: PEPE
#1: Other 47,41 %
#2: SNMP 33,97 %
#3: HTTP 15,59 %
#4: NETBIOS 2,7 %
06.09.2006 12:45:00 - 06.09.2006 13:00:00
Channel Volume Trend (91%)
1 Other 1192 kbytes 0
2 SNMP 853 kbytes 0
3 HTTP 392 kbytes 0
4 NETBIOS 68 kbytes 0
5 DNS 5273 bytes 0
6 ICMP 3802 bytes 0
Top Connections: PEPE
#1 2,63 %
#2 1,63 %
#3 1,51 %
#4 1,47 %
06.09.2006 12:45:00 - 06.09.2006 13:00:00
Source IP Source Port Destination IP Destination Port Protocol
1 10.0.0.222 1272 10.0.0.200 2208 TCP
2 10.0.0.230 138 (NETBIOS) 10.0.0.255 138 (NETBIOS) UDP
3 10.0.0.200 2208 10.0.0.222 1272 TCP
4 64.182.122.76 80 (HTTP) 10.0.0.200 1979 TCP
5 140.211.166.95 80 (HTTP) 10.0.0.200 1025 TCP
Port C&P on 10.0.1.126
5 min Averages - 60 Minutes
PAESSLER
V7.1.0.217 Netflow Edition LocalDev
132408 refreshs
33% CPU Load

Panels

In order to keep a better overview of your monitoring results PRTG offers the concept of “Panels”. Each panel can show one or more “Graphs” and “Tables” (see below) with various layout options.

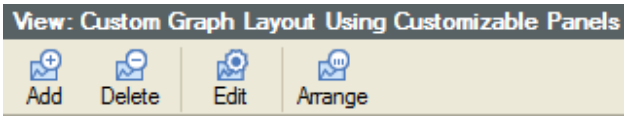
Panels are shown as “tabs” in the Custom Graphs view of the main window of PRTG Traffic Grapher:



Also, for the web interface, “Panels” are used for grouping the monitoring data, to control the layout in the web interface, and (optionally) to control access of different users to your monitoring results.

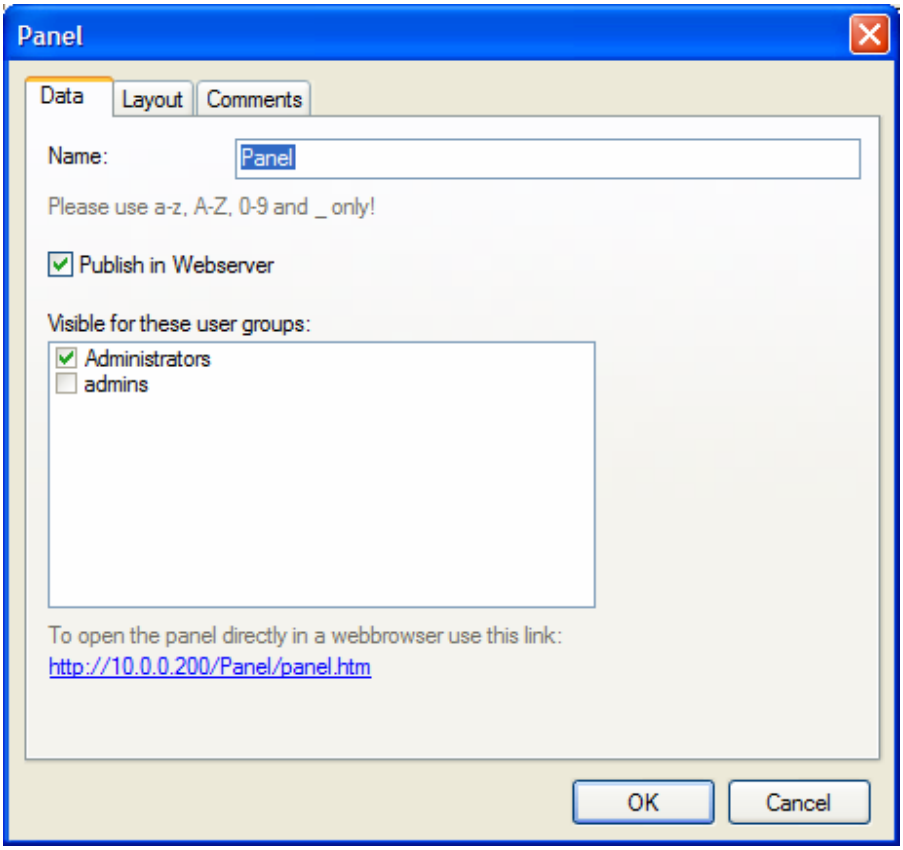
Working with Panels

If you choose the Custom Graph view you will see the toolbar for panels:



Adding Panels

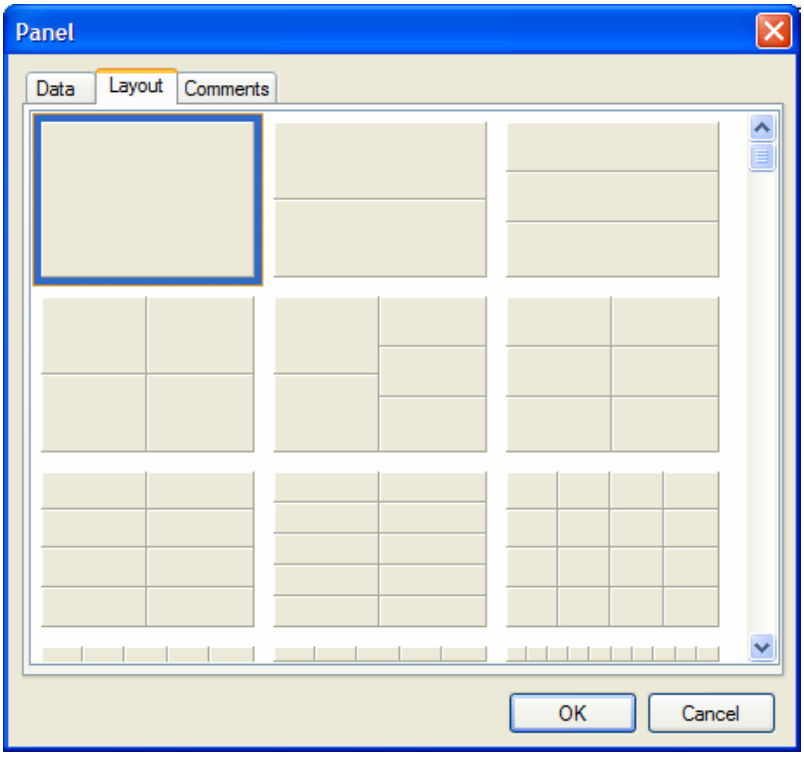
Click on **Add** to generate a new panel. Clicking this option opens up a new window. This window contains three separate tabs, **Data, Layout,** and **Comments**, described below.



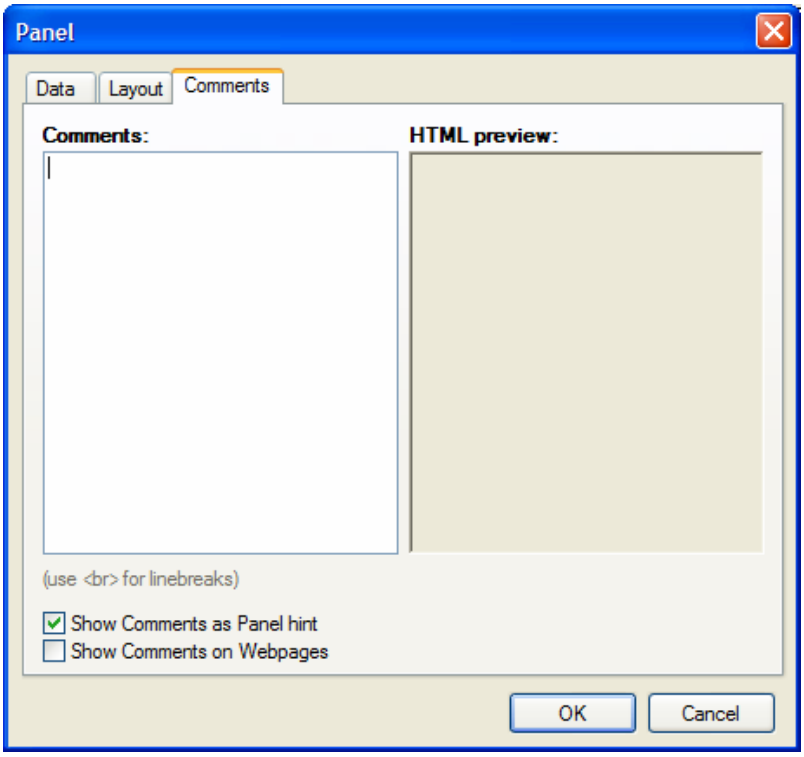
The **Data** tab allows you to set up the information pertaining to the panel. You can define the name for the panel (as it will be displayed on the panel tab in the main window). For this name only the characters a-z, A-Z, 0-9, and _ are allowed!

Check the checkbox **Publish in Webserver** if you would like this panel to be published via the web interface. You can also choose which user groups can access this panel.

At the bottom of this window, you will find a URL which will open the panel directly in the web browser.



On the **Layout** tab you can select a layout. Keep in mind, the distribution of the layout selected will also be mirrored by the information displayed on the web pages.



Finally the **Comments** tab enables you to enter a comment about this panel, which can optionally be shown in the web interface and the windows GUI.

Use simple HTML for highlighting, e.g. <b> for bold and <br> for line breaks.

In order to set up the new panel and its layout, please click the **OK** button.

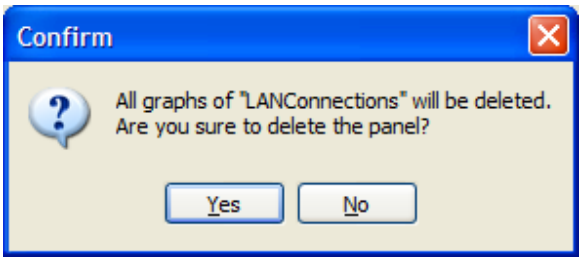
A new panel tab should appear among the existing panel tabs. Now you can create custom graphs by clicking on **Click here to add a new graph or table** as described later in the manual.

Editing Panels

The **Edit** button allows you to edit the settings of the panel. The options of this dialog are explained in the Adding Panels section.

Deleting Panels

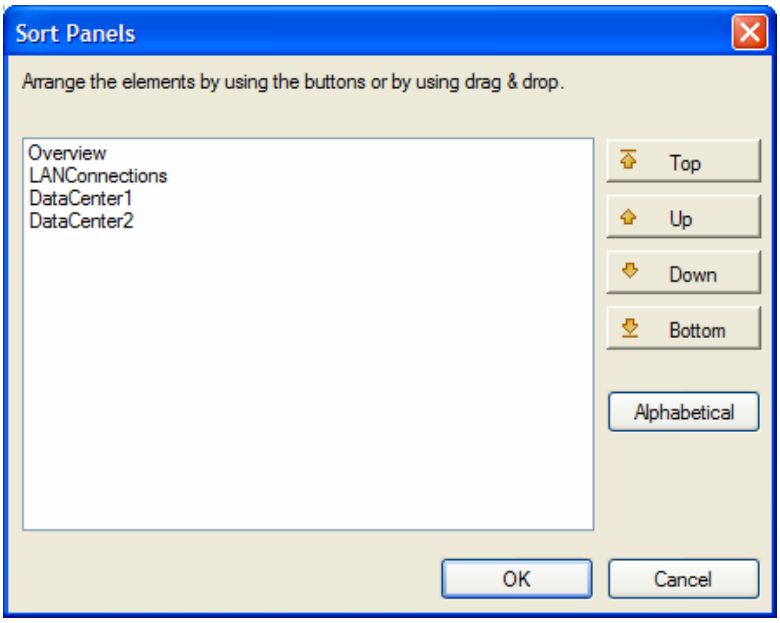
Selecting the **Delete** button will open a dialog asking whether the panel should be deleted or not. Once you delete a panel you can not recover it.



Should you wish to permanently delete this panel, click on **Yes**. Should you wish to keep the active panel, click on **No**.

Arranging Panels

The **Arrange** button allows you to manually sort the order of the panels and, thus, the sequence they will appear in the windows GUI and in the web interface.



Use the buttons to move panels up and down. You can also sort the panels alphabetically by clicking on the **Alphabetical** button.

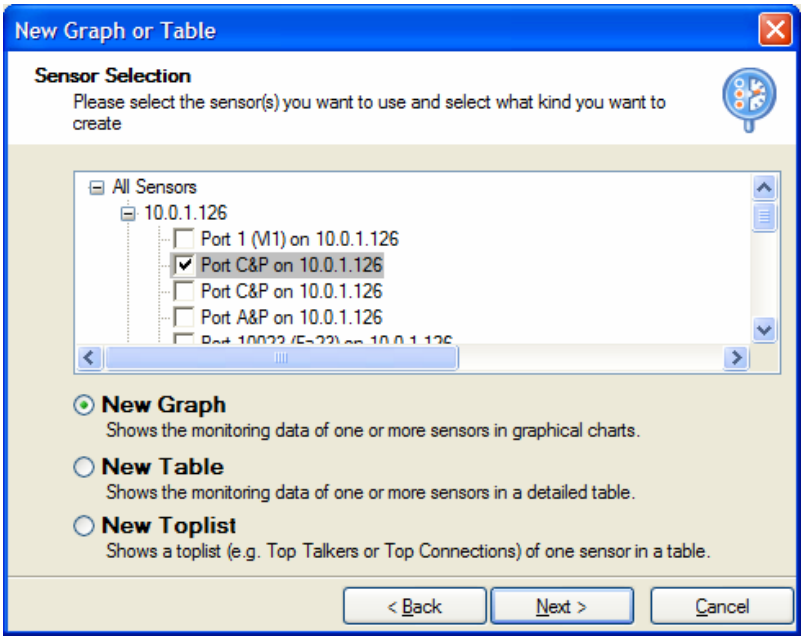
Adding Custom Graphs and Tables to a Panel

After creating a new panel you will see the button **Click here to add a new graph or table.** Click this button to create a new graph or table.

A wizard will show up:

New Graph or Table
Welcome to the Add Graph or Table Wizard
This wizard will guide you through the setup of a new graph or a new table that shows monitoring data of one or more sensors.
You will first have to choose one or more sensor(s) and then decide whether you want to create a chart or a table. Then you can change the options for this new item.
Please click "Next" to continue!
PAESSLER
< Back
Next >
Cancel

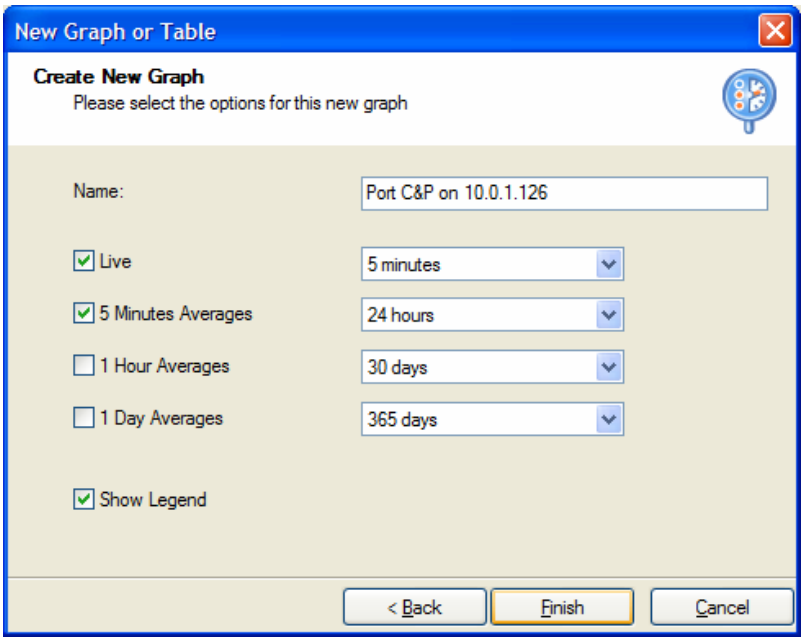
Click Next and you will see a list of all sensors:


New Graph or Table
Sensor Selection
Please select the sensor(s) you want to use and select what kind you want to create
All Sensors
10.0.1.126
Port 1 (M1) on 10.0.1.126
Port C&P on 10.0.1.126
Port C&P on 10.0.1.126
Port A&P on 10.0.1.126
New Graph
Shows the monitoring data of one or more sensors in graphical charts.
New Table
Shows the monitoring data of one or more sensors in a detailed table.
New Toplist
Shows a toplist (e.g. Top Talkers or Top Connections) of one sensor in a table.
< Back
Next >
Cancel

Select one or more sensors and decide whether to create a new graph, table, or toplist. Toplists are only available for Packet Sniffer and NetFlow sensors.

Creating a New Graph

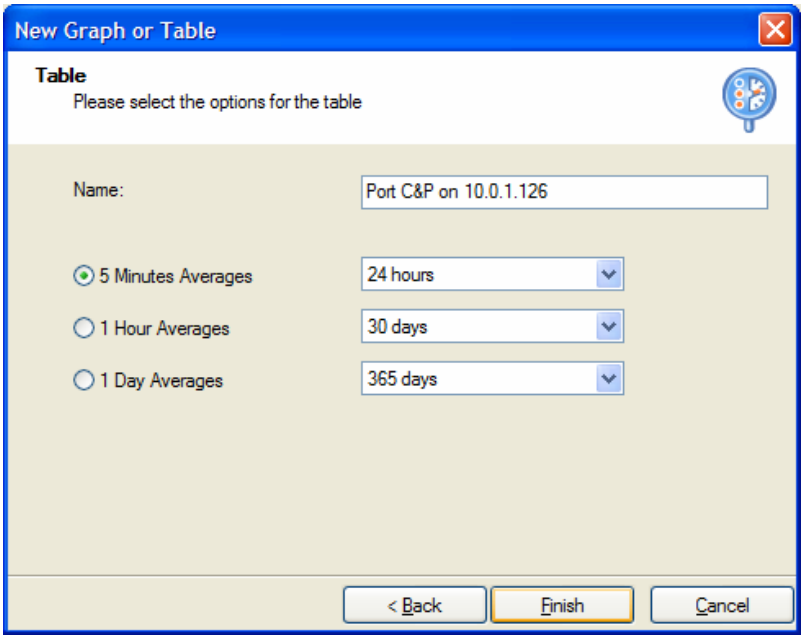
If you choose to create a new graph you have the following options:



Choose a name, enable the graphs you want, and set the graph's time frames. Click **Next** to finalize this step.

Creating a New Table

If you choose to create a new table you have the following options:



Choose a name, choose the averages to show on the table, and set the time frame. Click **Next** to finalize this step.

Creating a Toplist

If you choose to create a new toplist you can only give the toplist a new name. Click **Next** to finalize this step.

Working with Graphs and Tables

By clicking on the top of a graph or a table and holding down the mouse button you can drag and drop a graph from one position of the panel to another or even onto another panel. If you drop a graph onto another graph both will be swapped with each other.

At the top right of the graphs, one will find the buttons **Edit**, **Details**, and **Delete**.

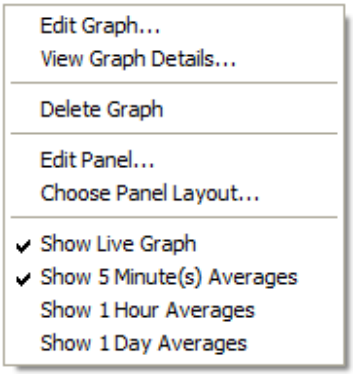
Opening Graph's or Table's Details

With a double click onto a graph or table or a click on the icon you can open a new window with detailed information. Please refer to the Working With Charts section.

Editing a Graph or Table

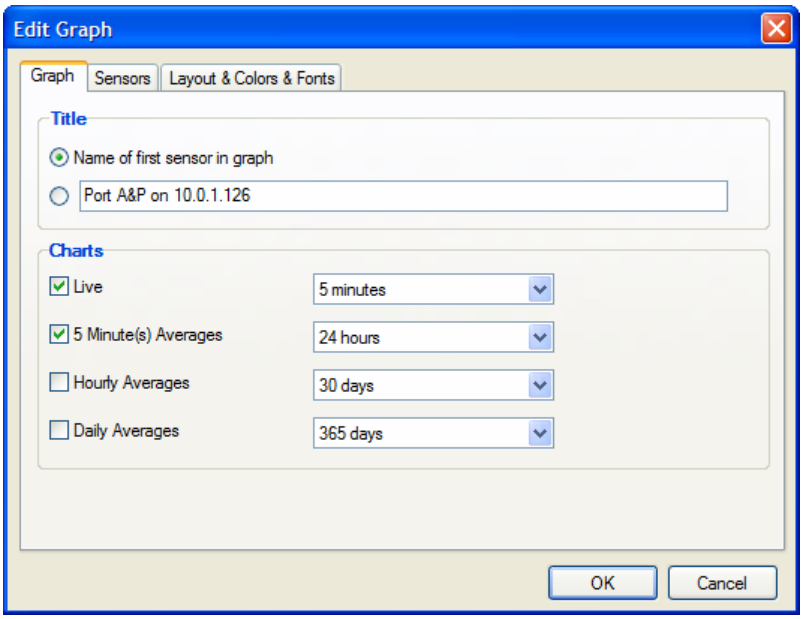
With a click on the icon located on the top right side of the graph you can edit a Graph or Table.

Another method to select this functionality is by selecting the **Edit Graph** option from the right-click menu.



The **Edit Graph** window allows for multiple changes to be made as regards the graphing function and its display. The **Edit Graph** window contains three panels:

- **Graph**
- **Sensors**
- **Layout & Colors & Fonts**



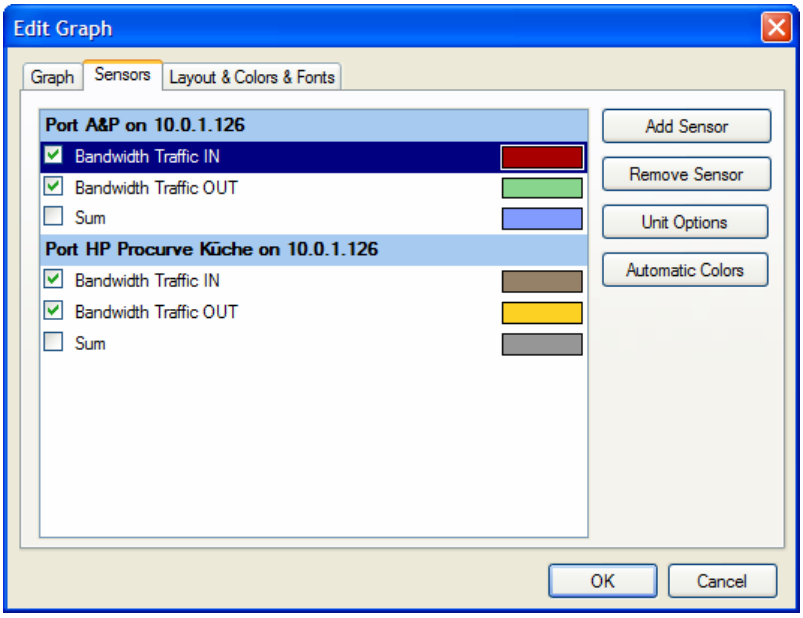
The first panel, **Graph**, is broken up into two sections, **Title** and **Charts**.

In the **Title** section, you can define the title given to the graph. You can either choose to use the name of the first sensor in the graph (which is the default setting). or enter a name of your choice that will replace the default.

In the **Charts** section, you can define the times you would like to use to display the graph information. The options are:

- **Live** – this will display real-time data capture, based on the time span defined in the drop-down menu to the right
- **x Minute(s) Averages** –this will display information based on 5 minute averages, over a time period defined in the drop-down menu to the right (the timespan depends on the custom intervals of the selected sensors).

- **Hourly Averages** – this will display information based on an hourly average, over a time period defined in the drop-down menu to the right.
- **Daily Averages** – this will display information based on a daily average, over a period defined in the drop-down menu to the right.



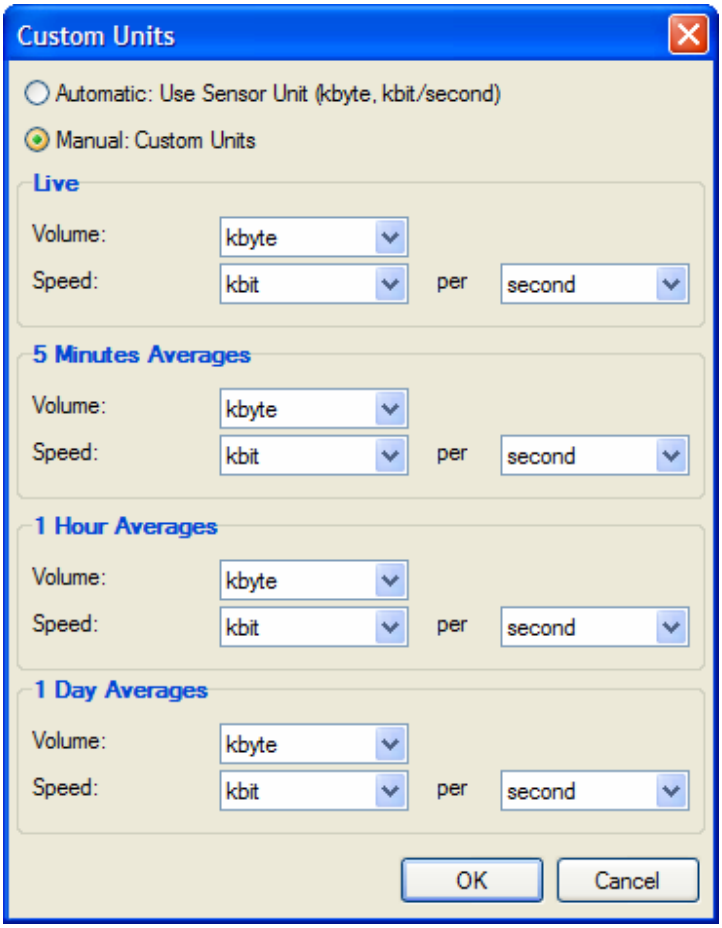
The second tab, **Sensors**, is broken up in various sections. The first section allows adding or removing a sensor by clicking the respective buttons, located on the right-hand side.

By clicking on the checkboxes it is possible to activate / deactivate the lines for each channel (e.g. Traffic IN, Traffic OUT, and others).

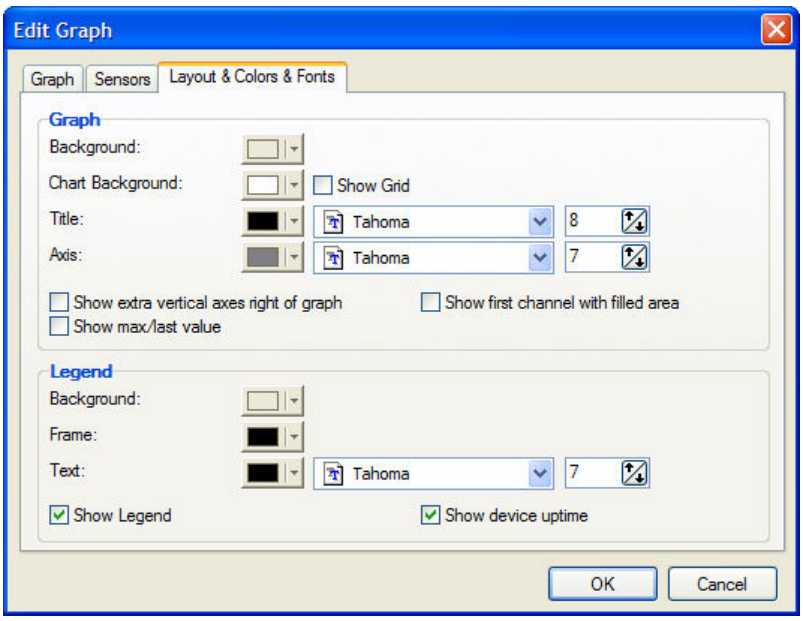
In this window, it is also possible to select the line colors for the channels by clicking on the appropriate color field. This will bring up a color selection: Simply click the color of your choice and click OK.

Optionally you can click on **Automatic Colors** and PRTG will automatically choose a unique color for each channel.

The button **Unit options** will open a new dialog allowing to select the various types of units for each of the selected graph types:



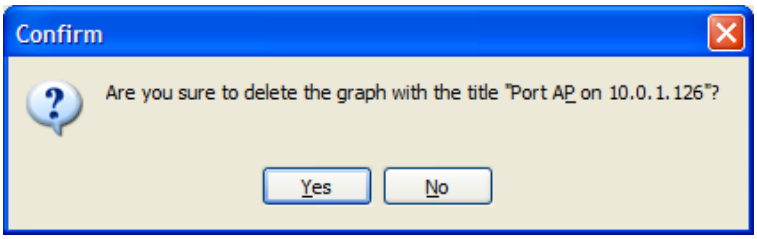
This dialog allows to select the units to be used for the volume and the speed of each entry, respectively.



The third tab allows you to change the **Layout & Colors & Fonts** displayed on the graph. Please see the section Change Colors & Layout for details.

Deleting a Graph or Table

When selecting the **Delete** button , a confirmation dialog will appear, asking whether you are certain you want to delete this graph.



Click **Yes** or **No**, depending whether you want to delete the graph or not.

Using the Web Interface

In order to properly understand the following section, please have a look at the **Basic Concepts** section at the beginning of this manual.

Concept

PRTG Traffic Grapher includes its own web server and allows the graphic information collected through the service to be accessed using a web browser from remote computers.

This feature can be used to give others in your LAN or even on the Internet access to you monitoring data.

Access to the monitoring data can be publicly accessible (the default) or can be limited to user accounts you can specify.

PRTG manages users in groups and, for each sensor and each panel, you can set specific access rights for these groups. The access policy, users and groups can be changed in the **Extras|Options** dialog.

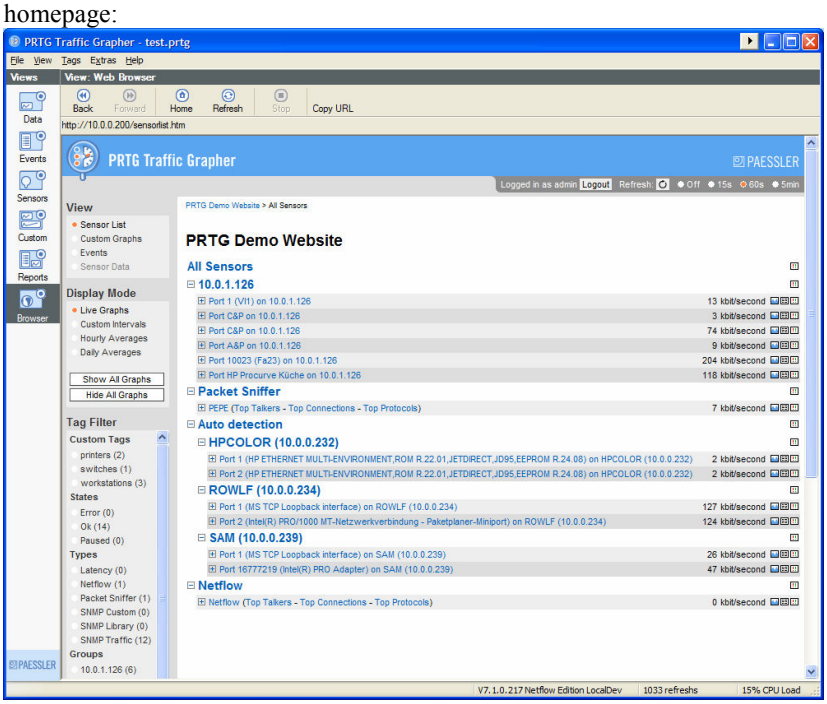
Accessing the Web Interface

You can access the web interface using the **Browser** view in the GUI of PRTG Traffic Grapher or you can use a standard web browser to access it.

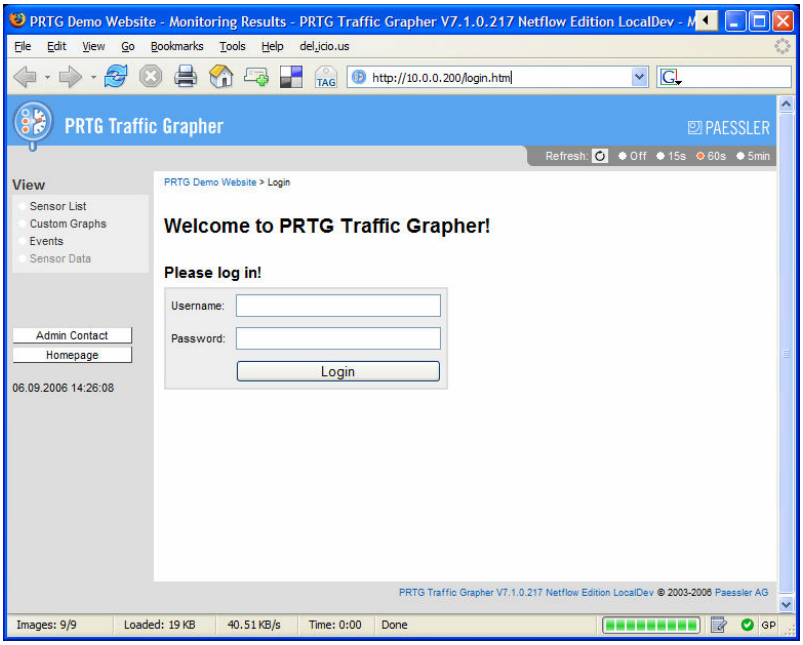
In order to access the web view with a web browser one must enter the appropriate URL on a remote computer. Note: The URL depends on the IP and port you have chosen in the web server settings in the **Extras|Options** dialog.

Note: You can also open the URL using the menu item **View|Open Web View in Browser**.

When switching to the Web Browser view in PRTG you will be taken to the homepage:



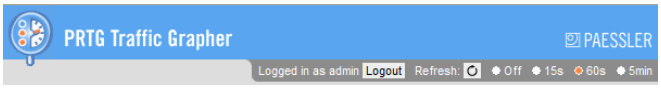
You may need to enter a username and password if you have enabled password protection. Note: You must enable cookies in your browser in order to log in.



Basic Layout of the Web Interface

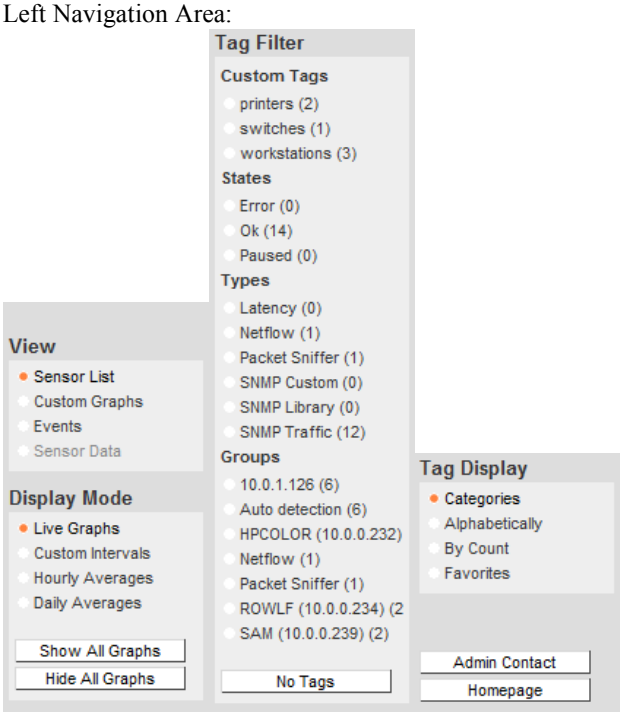
The layout consists of three main areas:

- Header Area:



In this area you can see the PRTG logo, the logout button, and controls for the page refresh.

- Left Navigation Area:

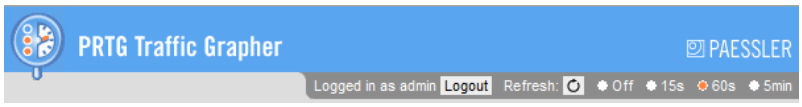


In this area you can control what data is shown.

- Data Area: The rest of the page contains the actual data which changes according to your settings in the navigation area.

Header Area

In this area of the web interface you have the following controls:



If you have selected password-protected access for the web server you will see the name of the user that is currently logged in. Click on **Logout** to log out and return to the login page.

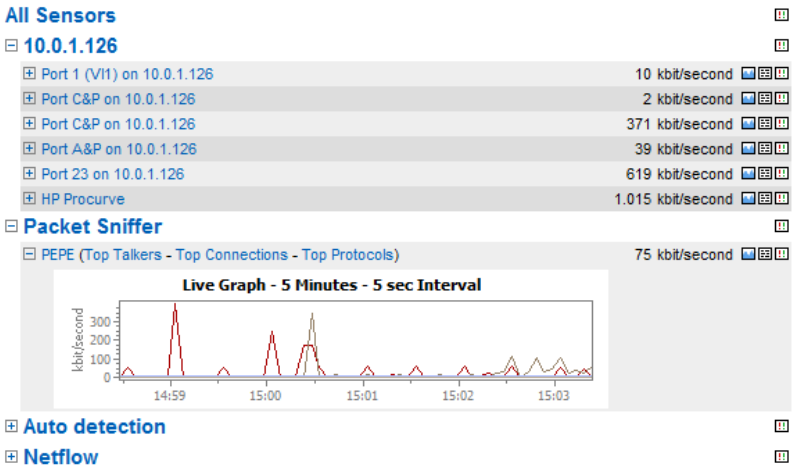
To refresh the page click on the corresponding button:

By default the page refreshes automatically every 60 seconds. Using the radio buttons you can also choose other intervals or deactivate automatic refreshes.

Note: If you want to use a refresh interval of your own choice please append the "timeout" parameter to the url with a value of the desired number of seconds, e.g. http://yourprtgserver/sensorlist.htm?timeout=240.

Sensor List View

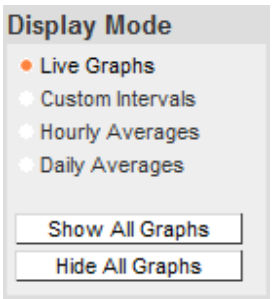
Choose Sensor List in the navigation area to see the list of sensors:



In this list you can use the following links:

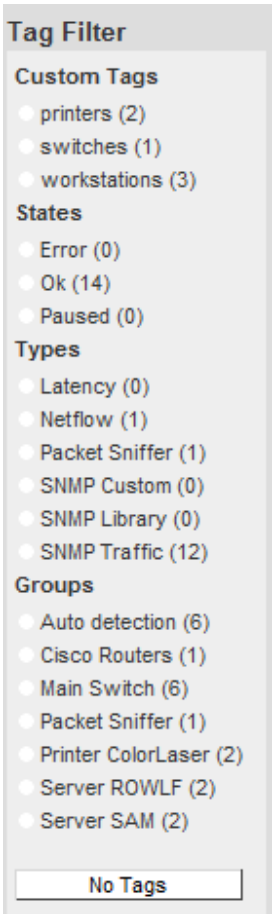
- Click the name of a group to get a page with only the sensors of this group.
- Click the Plus/Minus icons in front of group names to unfold/fold the group with its sensors
- Click the Plus/Minus icons in front of sensor names to show/hide the sensor's graph.
- Click a sensor name or the "graphs" icon to see the sensor's graphs in detail
- Click a sensor's "data table" icon to see the sensor's data in detail
- Click a sensor's or group's "events" icon and you will see a list of events for this sensor

You can change the graphs shown inside the list in the navigation area:



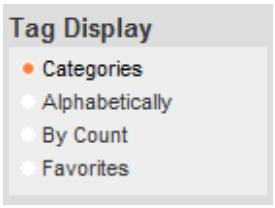
You can choose between **Live Graphs**, **Custom Intervals**, **Hourly Averages** and **Daily Averages**. Using the buttons **Show All Graphs** and **Hide All Graphs** you can hide and show all graphs at once.

You can filter the list of sensors using the Tag Filter:



Click one or more tags in the list and you will only get the sensors that have these tags associated in the list. Click on **No Tags** to return to the complete list.

You can also choose 4 different display options for the taglist:

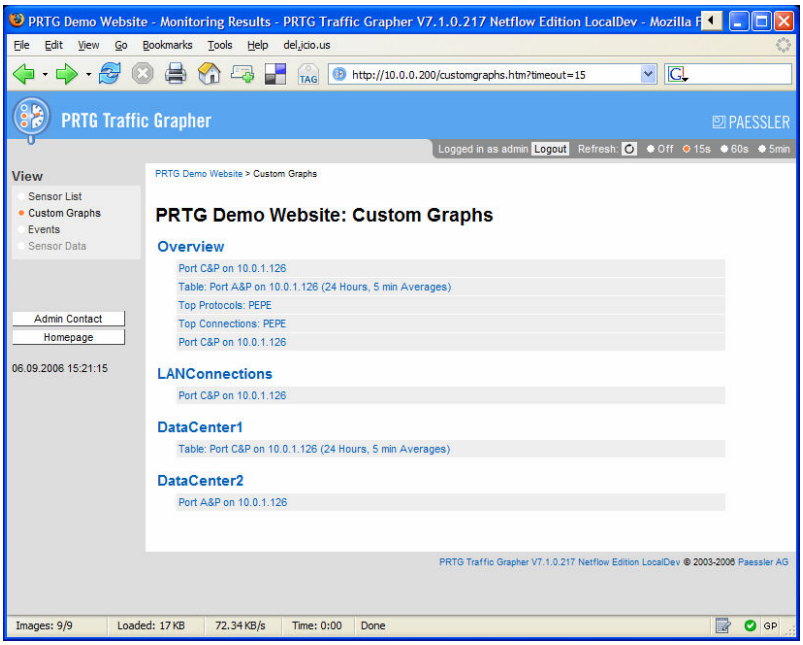


Note: Tag Favorites can be defined in the Windows GUI.

See the section Tags for details.

Custom Graphs View

Choose Custom Graphs in the Navigation bar to access the data of the custom panels through the web:

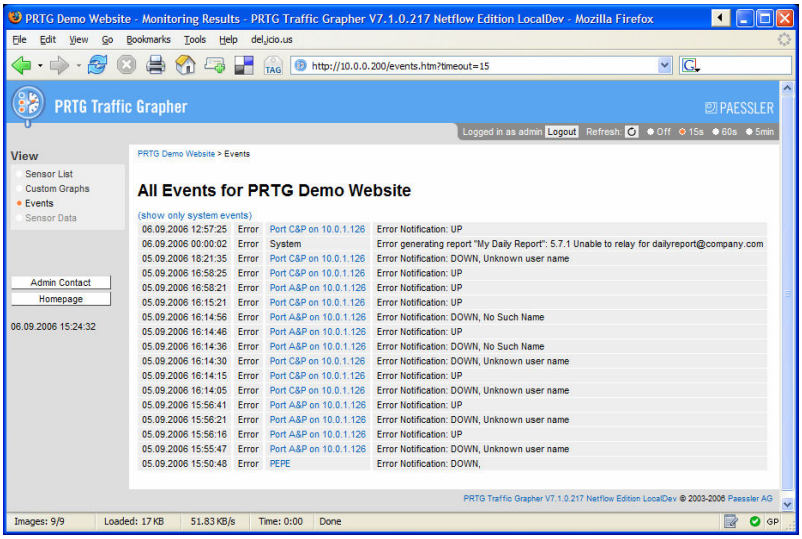


You will see a list of all panels defined in the Windows GUI. Click on a panel name to access the panel or click an item below that to directly jump to a graph or table.

See the section Working with Custom Graphs for details.

Events View

Choosing the option “Events” in the navigation bar will show you the list of all events:

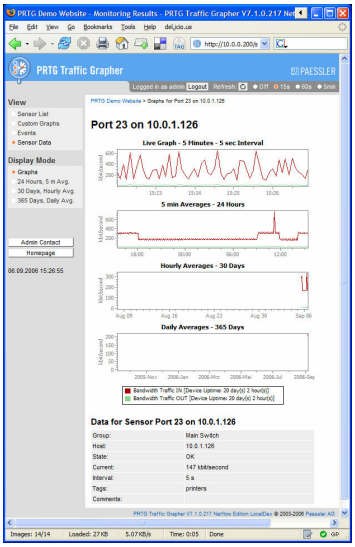

PRTG Demo Website - Monitoring Results - PRTG Traffic Grapher V7.1.0.217 Netflow Edition LocalDev - Mozilla Firefox
File Edit View Go Bookmarks Tools Help del.icio.us
http://10.0.0.200/events.htm?timeout=15
PRTG Traffic Grapher
PAESSLER
Logged in as admin Logout Refresh Off 15s 60s 5min
View
Sensor List
Custom Graphs
Events
Sensor Data
Admin Contact
Homepage
06.09.2006 15:24:32
PRTG Demo Website > Events
All Events for PRTG Demo Website
(show only system events)
06.09.2006 12:57:25 Error Port C&P on 10.0.1.126 Error Notification: UP
06.09.2006 00:00:02 Error System Error generating report "My Daily Report": 5.7.1 Unable to relay for dailyreport@company.com
05.09.2006 18:21:35 Error Port C&P on 10.0.1.126 Error Notification: DOWN, Unknown user name
05.09.2006 16:58:25 Error Port C&P on 10.0.1.126 Error Notification: UP
05.09.2006 16:58:21 Error Port A&P on 10.0.1.126 Error Notification: UP
05.09.2006 16:15:21 Error Port C&P on 10.0.1.126 Error Notification: UP
05.09.2006 16:14:56 Error Port A&P on 10.0.1.126 Error Notification: DOWN, No Such Name
05.09.2006 16:14:46 Error Port A&P on 10.0.1.126 Error Notification: UP
05.09.2006 16:14:36 Error Port A&P on 10.0.1.126 Error Notification: DOWN, No Such Name
05.09.2006 16:14:30 Error Port C&P on 10.0.1.126 Error Notification: DOWN, Unknown user name
05.09.2006 16:14:15 Error Port C&P on 10.0.1.126 Error Notification: UP
05.09.2006 16:14:05 Error Port C&P on 10.0.1.126 Error Notification: DOWN, Unknown user name
05.09.2006 15:56:41 Error Port A&P on 10.0.1.126 Error Notification: UP
05.09.2006 15:56:21 Error Port A&P on 10.0.1.126 Error Notification: DOWN, Unknown user name
05.09.2006 15:56:16 Error Port A&P on 10.0.1.126 Error Notification: UP
05.09.2006 15:55:47 Error Port A&P on 10.0.1.126 Error Notification: DOWN, Unknown user name
05.09.2006 15:50:48 Error PEPE Error Notification: DOWN,
PRTG Traffic Grapher V7.1.0.217 Netflow Edition LocalDev © 2003-2006 Paessler AG
Images: 9/9
Loaded: 17 KB
51.83 KB/s
Time: 0:00
Done

Click on **Show only System Events** to hide all events that are associated with a sensor.

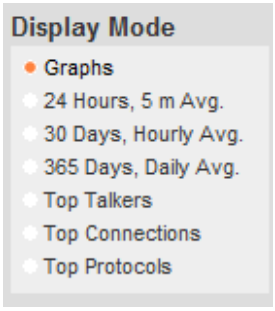
Note: To see the events for a sensor or group only use the icons in the sensor list.

Sensor Data View

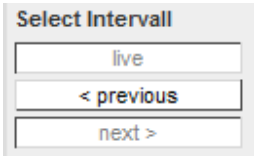
To review the graphs and settings for a sensor click the sensor's name in the sensor list:


PRTG Traffic Grapher
Port 23 on 10.0.1.126
Live Graph - 5 Minutes - 5 sec Interval
5 min Averages - 24 Hours
Hourly Averages - 30 Days
Daily Averages - 365 Days
Data for Sensor Port 23 on 10.0.1.126

In the navigation area you can now choose between the graphs and data tables:



When Toplists are shown you can change the currently shown interval with these links:



Creating Reports

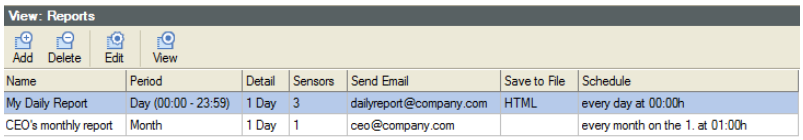
Reporting and Billing Concept

You can define an unlimited number of reports in PRTG Traffic Grapher. For each report you can individually choose various settings (e.g. the sensors which the report covers, the reporting interval). You can view the results of a report in the Windows GUI or optionally select to periodically write exports to a file on the disk or to periodically send them via email.

Additionally you can define billing schemes that can also be included in the reports.

Adding Reports

Switch to the Reports view to see a list of configured reports:

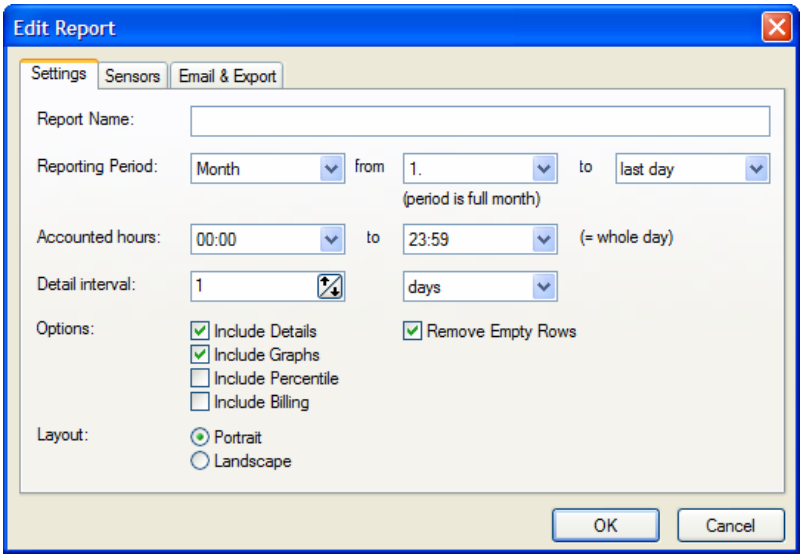


Name	Period	Detail	Sensors	Send Email	Save to File	Schedule
My Daily Report	Day (00:00 - 23:59)	1 Day	3	dailyreport@company.com	HTML	every day at 00:00h
CEO's monthly report	Month	1 Day	1	ceo@company.com		every month on the 1. at 01:00h

Click on **Add** to create a new report. A window comes up where you can edit the settings for the report as described in the following Editing Reports section.

Editing Reports

To edit a report choose the report in the list and click on **Edit**.



This dialog has three tabs: **Settings**, **Sensors,** and **Email & Export**.

Settings

First please enter a **Report Name** which should be chosen to uniquely identify this report.

Then choose a **Reporting Period**: You can have daily, weekly, monthly, and yearly reports. You can also choose the beginning and ending point of the period.

If you do not want the accounting to cover the whole 24 hours of a day you can choose any other timeframe for the **Accounted Hours**, as well.

The Detail Interval allows you to define the granularity of the data table, e.g. hourly for a daily report or daily for a monthly report (**Include Details** must be enabled).

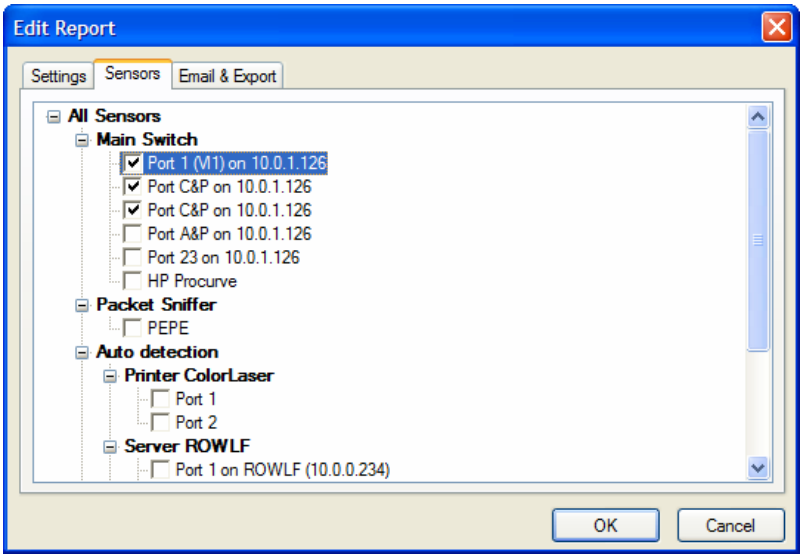
Next please enable or disable the optional parts of the report:

- **Include Details:** This shows additional data in the report, e.g. daily data for a monthly report.
- **Include Graphs:** This setting will include a graph of the data in the report
- **Include Percentile:** Enable this setting if you want to have the percentile calculated in this report (please choose the percentile value (e.g. 95%) in the **Extras|Options** dialog).
- **Include Billing:** This setting will cause the report to show the billing results, if a pricing scheme has been selected in the sensor's settings.
- **Remove Empty Rows:** If table cells do not contain data they will be hidden in the report.

Finally you can choose to have a **Portrait** or **Landscape** paper orientation.

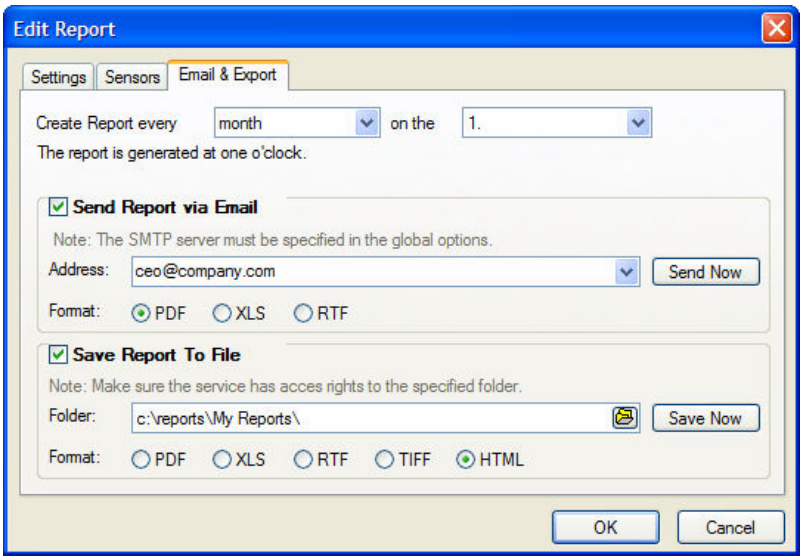
Sensors

Please choose the sensors that the current report should include by checking the box in front of each sensor item.



Email & Export

This tab allows you to create reports periodically.



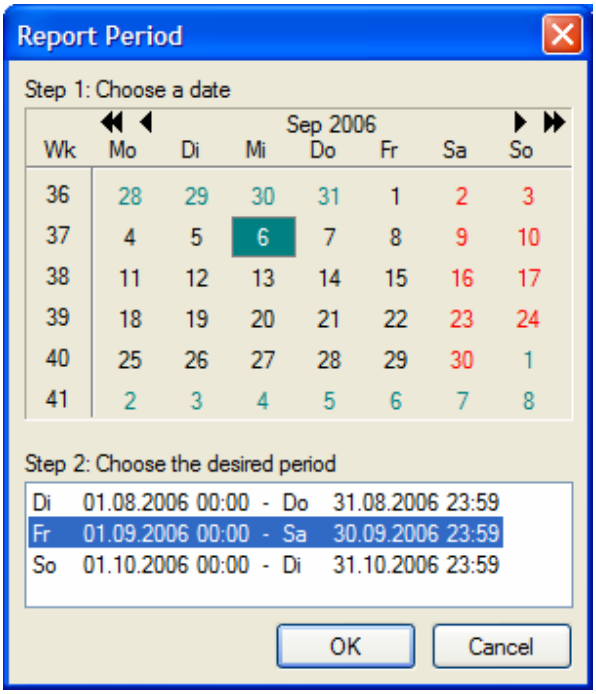
The first setting allows to define the time when the report should be created. The available options depend on the report interval.

Enable **Send Report Via Email** to send an email with the report whenever the point in time chosen above occurs. The report will be attached to the email according to your choice as a PDF, XLS or RTF file. Click on **Send Now** to send an email with the report immediately.

Enable **Save Report to File** and you will get a new report every day/month/year (depending on the Reporting Period Setting) in the folder that you specify. You can choose between various file formats. Click on **Save Now** to write a report to the folder immediately.

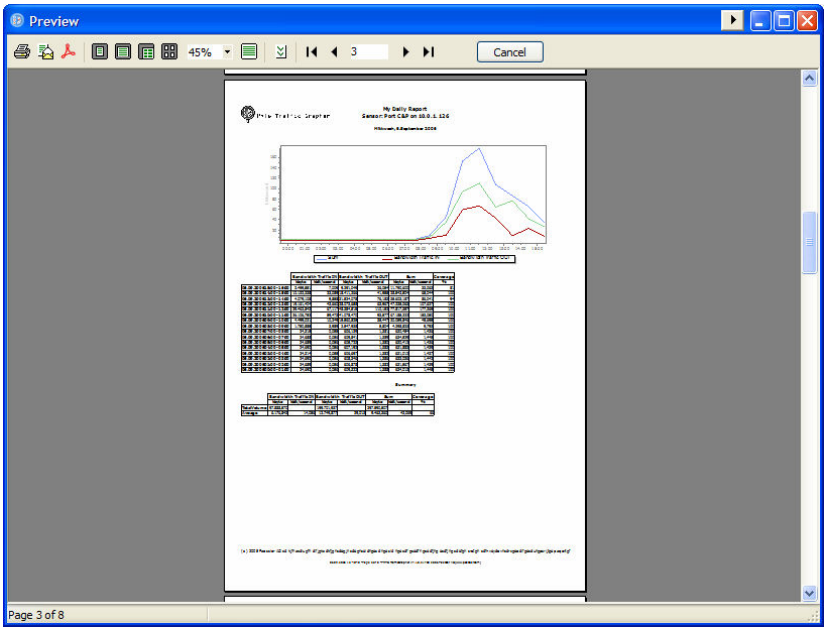
Viewing Reports

To view a report, select the report and click **View** or double click a report. Now you have to define the point in time that should be used for the report:



First use the calendar to choose a date then select a interval in the lower list. Finally click OK.

After a few moments the report will show up:

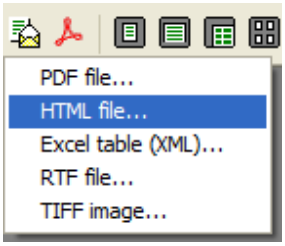


Using the toolbar you can print and export the report, change the zoom factor, use the full screen for viewing, edit the layout settings, and change the current page.

Click on **Cancel** to close the report.

Exporting Reports to PDF, HTML, Excel, RTF, and TIFF

Click on the Export Logo and then choose the file format of your choice:



Depending on the file format you have several options.

You may want to change some of the settings here, but for most situations the presets should be fine. Click **OK** and then specify a folder and a filename. A few moments later your default file viewer will start and show the report.

Reading Reports

Reports can include the data of one or more sensors. For each sensor the report consists of several sections:

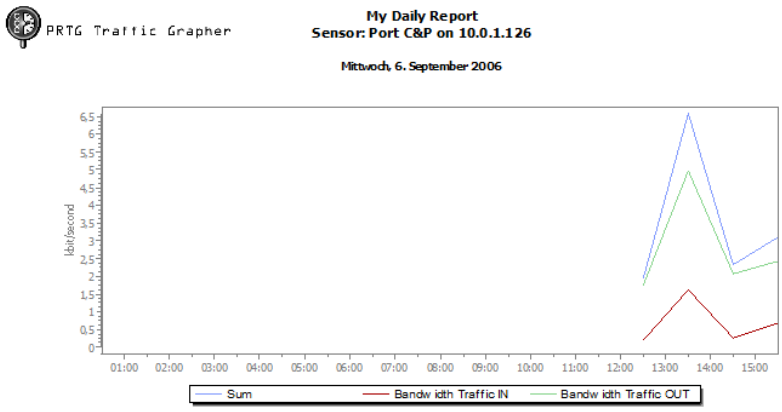
- Graph (if enabled)
- Detailed data table (if enabled)
- Summary

All pages show a logo in the top left corner and the name of the report and the name of the sensor.

Note: The top-left logo, the footer line, and the report font can be changed in the **Extras|Options** dialog.

Graph

The graph section shows the graph for one sensor and uses the standard graph settings as set in the **Extras|Options** dialog.



Detail Data

The detail data section shows the data of the sensor with various columns. If percentile is enabled in the report's setting then also a column is shown with these values.

	Bandwidth Traffic IN		Bandwidth Traffic OUT		Sum		Coverage
	kbyte	kbit/second	kbyte	kbit/second	kbyte	kbit/second	%
06.09.2006 15:00 - 16:00	282,214	0,693	988,298	2,425	1.270,512	3,118	93
06.09.2006 14:00 - 15:00	116,539	0,266	905,874	2,064	1.022,413	2,330	100
06.09.2006 13:00 - 14:00	669,348	1,621	2.051,952	4,970	2.721,300	6,591	94
06.09.2006 12:00 - 13:00	3,633	0,192	32,870	1,738	36,503	1,930	4

Summary and Billing Data

The last section of a report for a sensor is the summary which also includes the billing data, if billing is enabled for this report and if there is a pricing scheme set for the sensor in the sensor's settings.

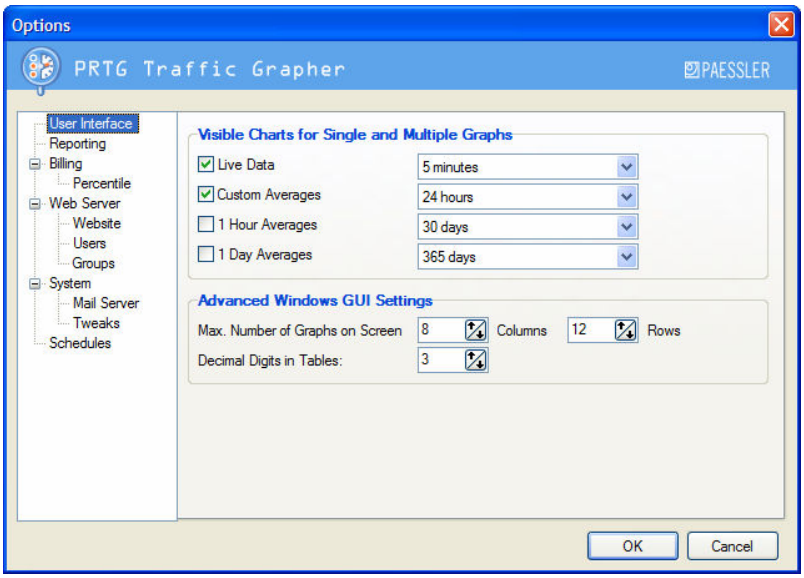
Summary

	Bandwidth Traffic IN		Bandwidth Traffic OUT		SUM		Coverage
	kbyte	kbit/second	kbyte	kbit/second	kbyte	kbit/second	%
Total Volume	70.501.606,61		19.629.533,48		90.131.140,09		
Average	2.279.939,97	216,17	634.796,40	60,19	1.457.368,18	276,36	100
95th Perc. (5 min)		509,64		205,88		523,84	
Base Charge						99,95 $	
Percentile Charge						0,00 $	
Volume Charge						523,84 $	
Sum Charge						623,79 $	

Setting Program Options

Selecting the menu item **Extras|Options** opens the **Options** dialog. From here, you have the ability to select one of the tabs to change the settings for various parts of the program. The following sections will cover these individual settings in detail.

User Interface Settings

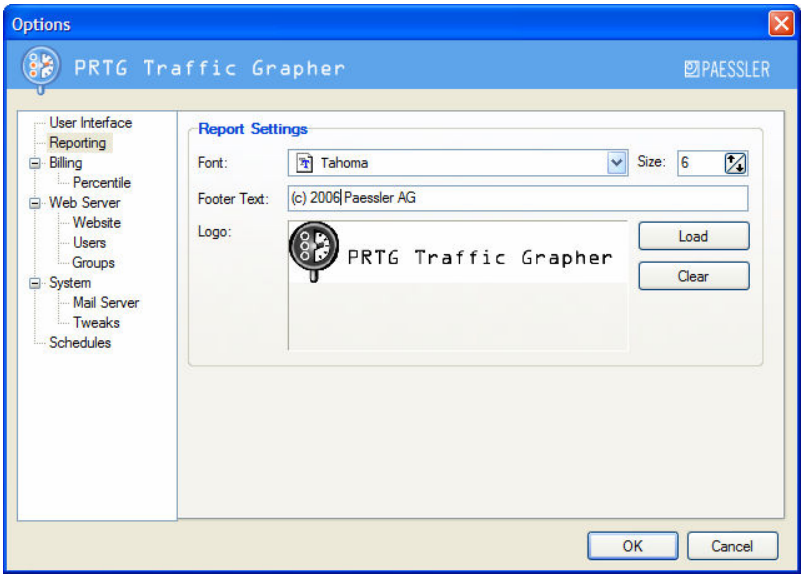


On this tab you can select which charts with what time frame are shown throughout the program and the web interface (except for the Custom Panels).

To avoid slow windows refreshes for large installations with hundreds of sensors or more PRTG limits the number of sensors shown in the Data view to the number that you set with **Max Number of Graphs on Screen**. The default setting of 4 by 4 (=16) graphs can be adjusted as you like.

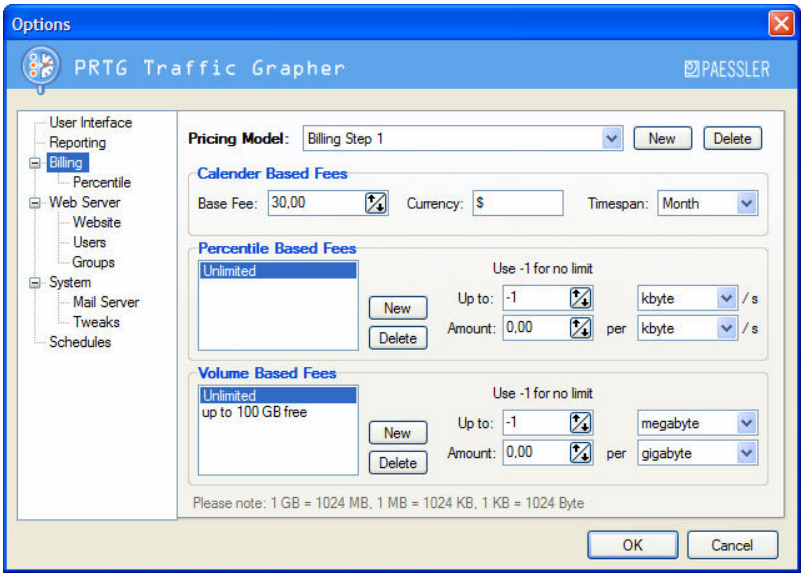
For data tables in the Windows GUI, Web interface, and in the reports you can also set the number of **decimal digits**.

Reporting Settings



Use this tab to select the font and font-size, the footer text, and the logo image for reports.

Billing Settings



If you want to use PRTG to calculate bills for your customers you must set up the pricing models here. The price can consist out of three parameters:

- Base Fee: This value is charged once per timespan
- Percentile Based Fees: Based on the percentile you can enter several charge steps.

- Volume Based Fees: Based on the transferred volume of data you can enter several charge steps.

Note: You must select a pricing model for each sensor in the sensor settings.

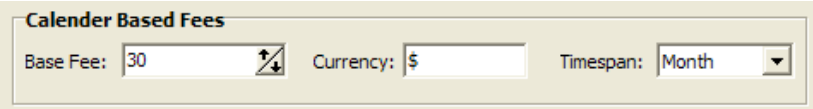
How to Set up a Pricing Model

In this sample we create a billing model with the following parameters:

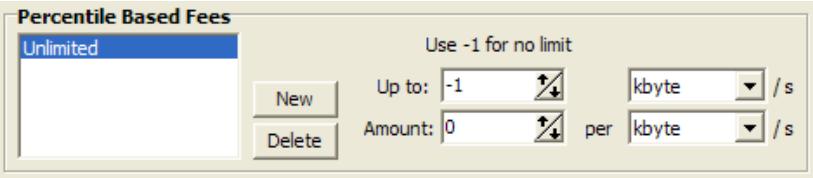
- Monthly base fee: $30
- Volume of 100 GB included
- $2,50 per GB for volume exceeding 100 GB

First you need to create a new pricing model. Click on **New**:

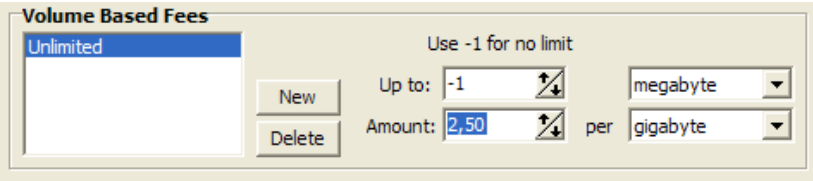
In the **Calendar Based Fees** section enter the monthly base fee of $30 in the **Base Fee** field and set your desired **currency** string.



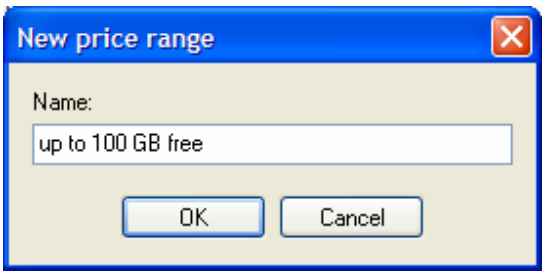
Since we do not want percentile based billing we enter an **amount** of 0 in the **Percentile Based Fees** section.



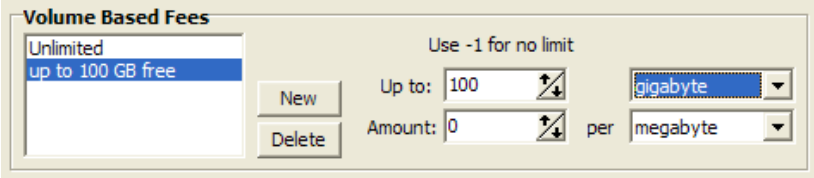
In the Volume Based Fees section we need to make the following changes: To charge 2,50 per GB we need to enter 2,50 for the **Amount** of the **unlimited** setting and we need to choose **per gigabyte**:



To make the first 100GB free we create a new item by clicking **New** and entering a name for the new item:



For this new item we change the **Up To** value to the value of 100 GB and enter the value of 0 for the **Amount**:

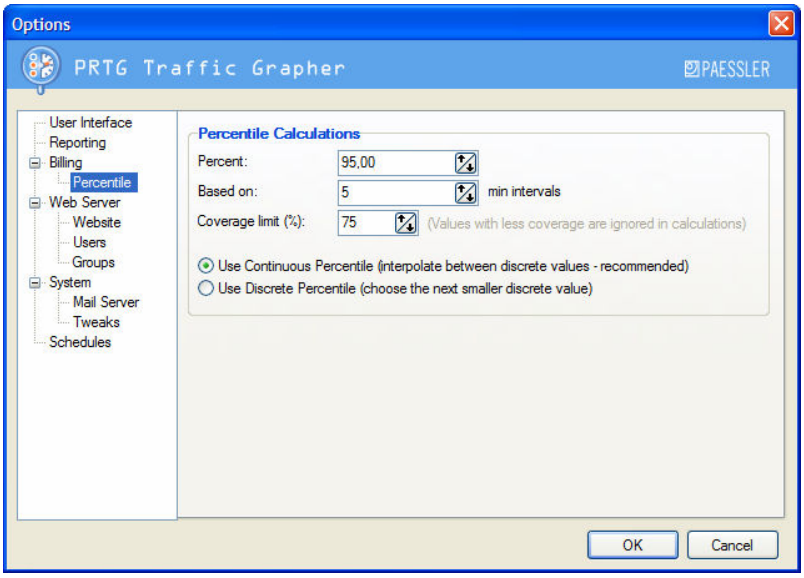


That's all. Now you must edit all sensors and choose this pricing model billing on the Billing tab of the edit sensor dialog.

If all these steps are done you can create new reports and they will contain the billing data when you enable billing for a report.

Percentile Settings

If you want to use percentile calculation you must enter your desired values here:



Please enter your values for **Percent** and your desired intervals.

The **coverage limit** should also be set to avoid that the calculation is incorrect in the case PRTG's monitoring is stopped for a short time.

Continuous percentile interpolates between discrete values (this is the recommended setting), whereas discrete percentile chooses the next smaller discrete value.

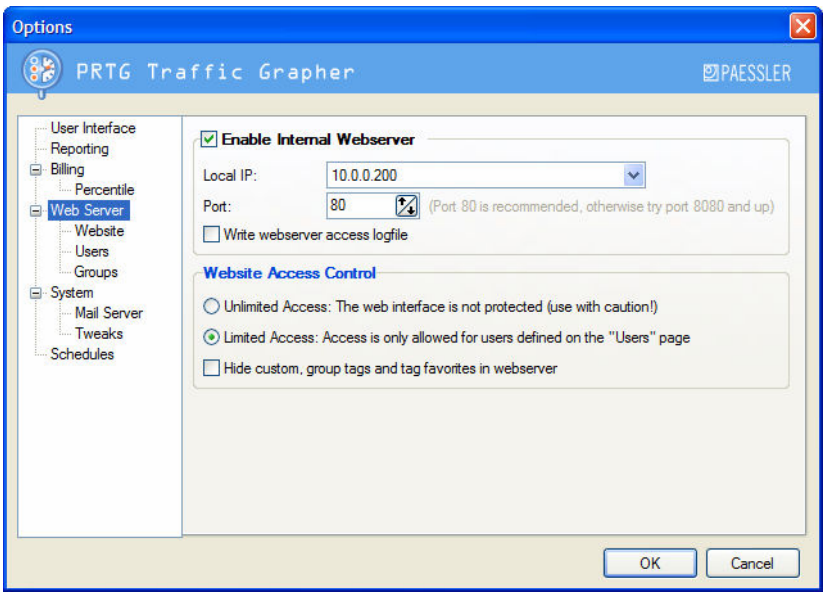
Continuous percentile basically means that the measurements are treated as a statistical population and the value is determined by interpolating a value when it isn't present. This means that values are interpolated between actual measurements that are varying around the „perfect" center of the measurements.

Discrete percentile means that the value must be a member of the data set. For this kind of calculation you require a discrete distribution. The median of a discrete distribution can not be defined, as such, meaning that the 50th discrete percentile may not necessarily be the median if the value does not belong to an odd number of measurements. Discrete percentiles, as such, should not be used for billing applications.

A good source for more information regarding these percentiles can be found on this page: http://www.servicelevel.net/rating_matters/newsletters/issue13.htm

Web Server Settings

The **Web Server** tab allows to set up the web server functionality.



You can enable / disable the internal web server by checking / unchecking the **Enable Internal Webserver** checkbox.

You can also define the **Local IP** address, as well as the **Port**. Usually port 80 is used for web server, but if this port is already used on your machine the second choice would be port 8080. Of course, any other desired port can be selected as long as it is not already being used by other applications.

If you also have other web servers running on the machine that you run PRTG Traffic Grapher on you must keep in mind that each port number can only be used by one server!

The option **Write webserver access logfile** generates a subdirectory entitled "weblog" in the data folder which contains an *.log file with the data access information of the web server in W3C format (see http://www.w3.org/TR/WD-logfile.html).

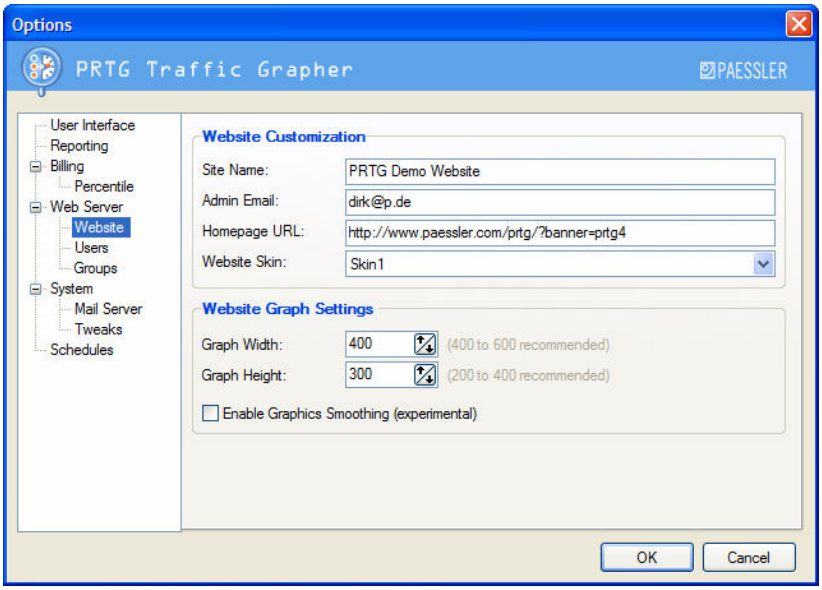
For **Website Access Control** you have two options:

- Unlimited Access: All data in the web interface can be accessed without any login, etc.
- Limited Access: Only users defined on the users page can log into the website.

For each sensor and each panel you can define what user groups can access their data.

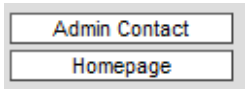
Website Settings

The **Web Site** tab allows to specify certain functions as regards the web interface.



This will affect the way that the web view will be displayed

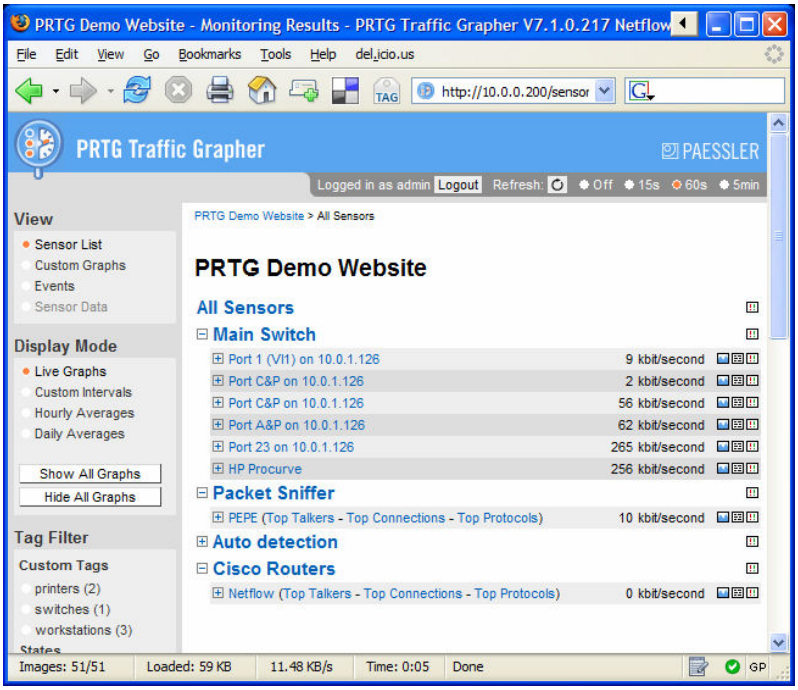
It is possible to define a **Site name** (this will be displayed at the start of the web view, where one can select the monitored sensors), an **Admin email** and a **Homepage URL**. The administrator email, as well as the defined homepage URL will be available as links in the bottom left hand of the web view.



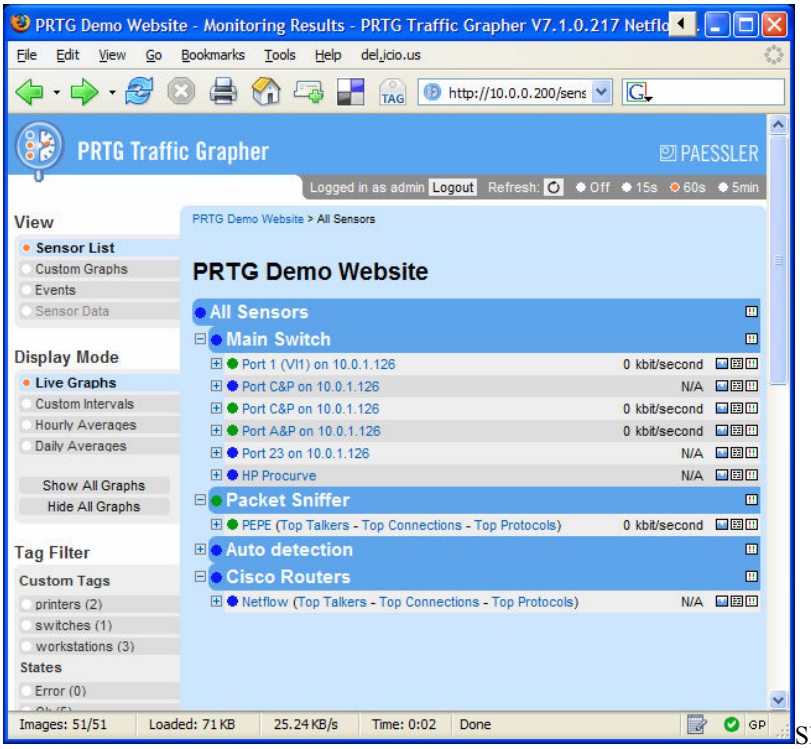
You can also select one of various skins to change the look and feel of the web interface. Please use the drop down menu to select the desired skin.

PRTG comes with three pre-defined skins. You can also edit the skins, see the appendix for details.

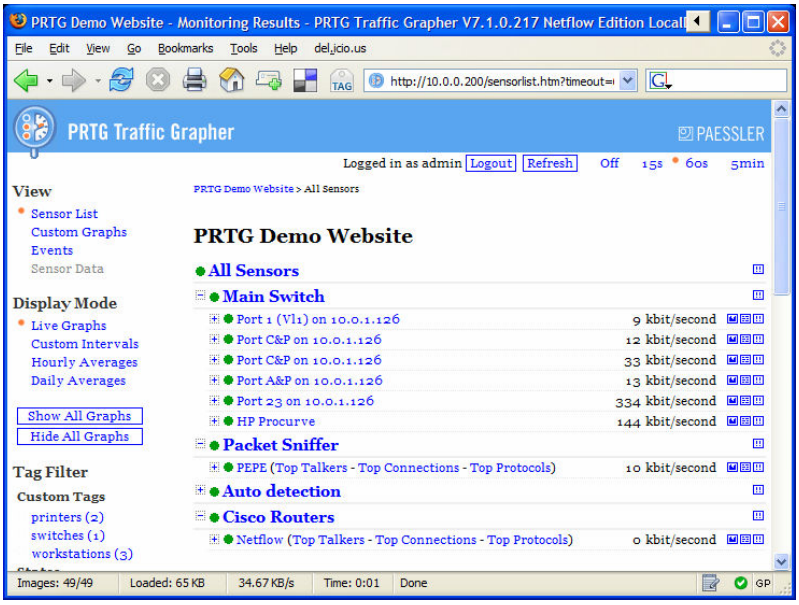
“Skin 1” is the default skin:



Skin 2 looks a little heavier and features rounded corners. It is not well suited for more than 50-100 sensors:



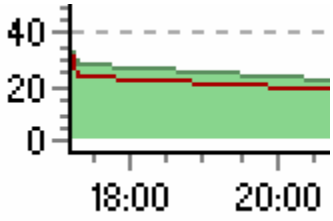
Skin 3 is a minimal graphics skin on a white background:


PRTG Demo Website - Monitoring Results - PRTG Traffic Grapher V7.1.0.217 Netflow Edition Locall
File Edit View Go Bookmarks Tools Help del.icio.us
http://10.0.0.200/sensorlist.htm?timeout=
PRTG Traffic Grapher
PAESSLER
Logged in as admin Logout Refresh Off 15s 60s 5min
View
Sensor List
Custom Graphs
Events
Sensor Data
Display Mode
Live Graphs
Custom Intervals
Hourly Averages
Daily Averages
Show All Graphs
Hide All Graphs
Tag Filter
Custom Tags
printers (2)
switches (1)
workstations (3)
PRTG Demo Website > All Sensors
PRTG Demo Website
All Sensors
Main Switch
Port 1 (Vl1) on 10.0.1.126 9 kbit/second
Port C&P on 10.0.1.126 12 kbit/second
Port C&P on 10.0.1.126 33 kbit/second
Port A&P on 10.0.1.126 13 kbit/second
Port 23 on 10.0.1.126 334 kbit/second
HP Procurve 144 kbit/second
Packet Sniffer
PEPE (Top Talkers - Top Connections - Top Protocols) 10 kbit/second
Auto detection
Cisco Routers
Netflow (Top Talkers - Top Connections - Top Protocols) 0 kbit/second
Images: 49/49 Loaded: 65 KB 34.67 KB/s Time: 0:01 Done

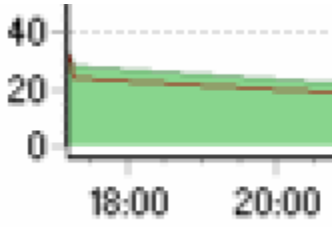
The **Web Interface Graph Settings** section allows you to enter the **graph width** and the **graph height**, as they will be shown in the web view. Keep in mind – if you enter very high values, the graphs may spread beyond the limits of the web browser's window size. However, you will still be able to scroll the extents of the graphs, albeit rendering the graphs and transferring the data will take much longer than with normal values.

The checkbox **Enable Graphics Smoothing (experimental)** will allow to anti-alias (smooth) the jaggy edges of the graph and fonts in the web view. As such, a clearer image without annoying "steps" will appear (see images below).

It is a very subjective question whether to use Graphics Smoothing or not. Please note that using Graphics Smoothing creates a higher CPU load when graphs are computed.



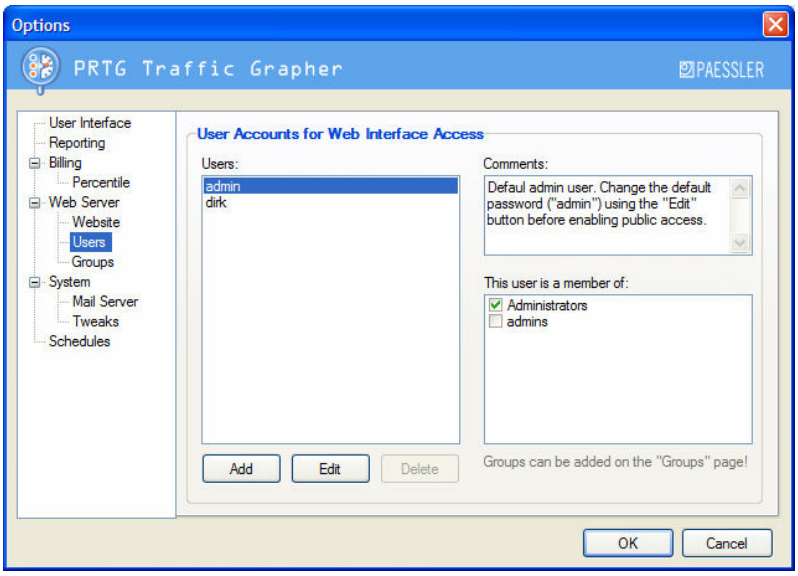
Without smoothing (zoomed to 200%).



With smoothing (zoomed to 200%).

Web Server User Settings

Here you can edit the user accounts that can access the web interface (if you disable public access).

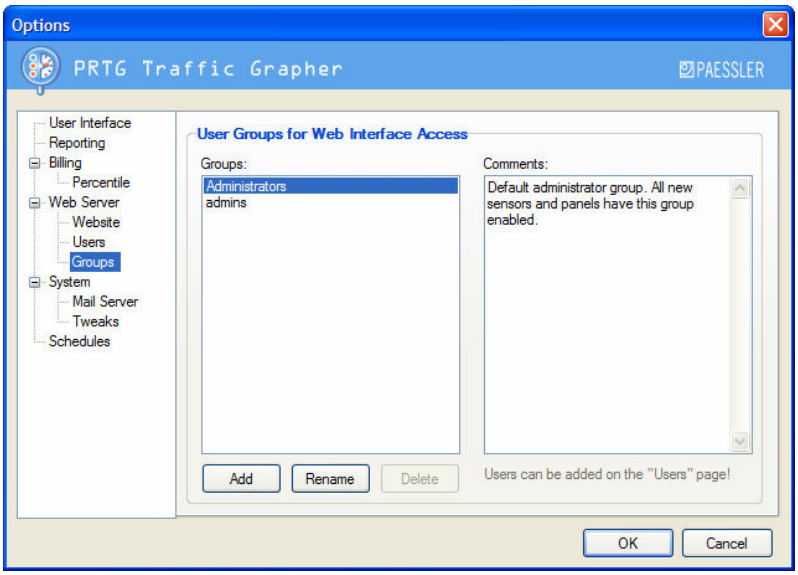


Click on **Add** to create new accounts, use **Edit** and **Delete** to work with the accounts. You can also enter **Comments** for each user.

Make sure that each user is member of at least one group (by checking the boxes to the left of the group names) since you can only define the access on group level for sensors and panels.

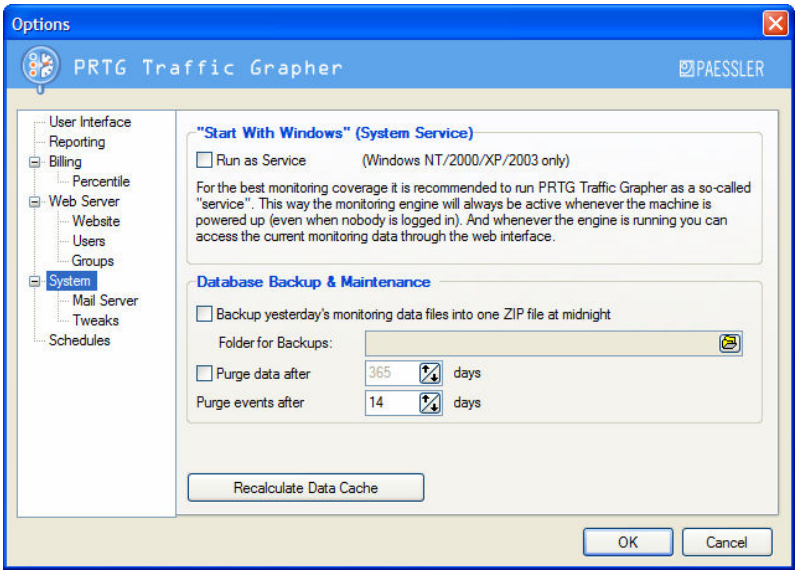
Web Server Group Settings

Use this screen to manage groups.



Click on **Add** to create new groups, use **Edit** and **Delete** to work with the groups. You can also enter **Comments** for each group.

System Settings



In the **Start with Windows** section, you can define whether the program is to run as a service (under Windows 2000/XP/2003 only).

Running a program "as a service" means that the program is always run when the computer is powered on, regardless of somebody being logged on or not. Only this way can it be ensured that monitoring is running all the time, which is necessary to cover 24 hours each day.

If this checkbox is checked the program will continue operating as a "service" even when you close the Windows GUI or log off from your Windows machine. It will also start monitoring immediately after powering on your machine.

It is strongly recommended to use this feature to ensure 100% coverage of your monitoring!

In the **Database Backup & Maintenance** section you can change database parameters:

You can choose to do a daily backup of the monitoring data by enabling **Backup yesterday's monitoring data…** and providing a folder for the backup.

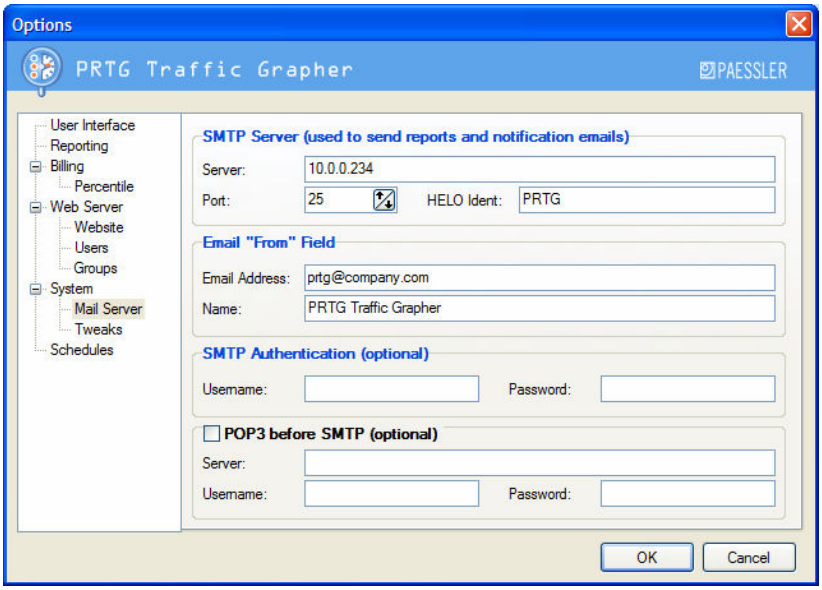
Using the backup function will give you a zipped file containing all collected monitoring data for a particular day. The backup for the previous day will be created as soon as a new day begins.

To keep the database from growing endlessly you can also enable **Purge data after** and choose a number of days that PRTG should keep the data in the database.

To avoid memory overload you should keep the list of events only for a few weeks. You can choose the number of days in the **Purge events after** setting.

Mail Server Settings

In order to send emails PRTG Traffic Grapher must be given information about your mail server.



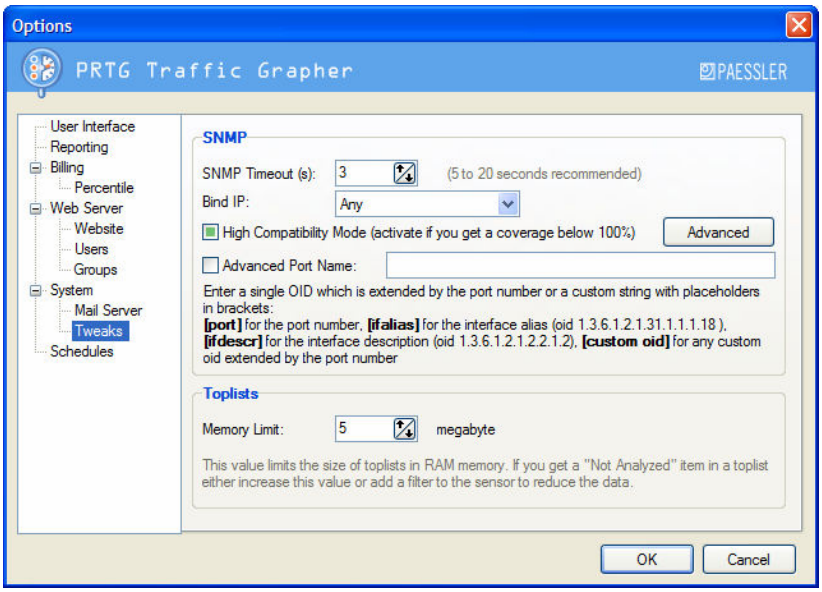
The **SMTP Server** section allows you to enter the server information, the port number, and a HELO id used to connect to the mail server.

The **Email "From" Field** section allows to enter the email address and the name you would like to appear in the "from" section of all emails sent by PRTG Traffic Grapher.

The **SMTP Authentication** section allows you to enter a username and password in order to authenticate the transfer of the email information on your SMTP server. Please make sure this information is provided accurately, as otherwise the authentication process will not work properly.

If your mail server requires **POP3 before SMTP** you must enter your account data in the edit fields provided.

Tweaks Settings


Options
PRTG Traffic Grapher
PAESSLER
User Interface
Reporting
Billing
Percentile
Web Server
Website
Users
Groups
System
Mail Server
Tweaks
Schedules
SNMP
SNMP Timeout (s):
3
(5 to 20 seconds recommended)
Bind IP:
Any
High Compatibility Mode (activate if you get a coverage below 100%)
Advanced
Advanced Port Name:
Enter a single OID which is extended by the port number or a custom string with placeholders in brackets:
[port] for the port number, [ifalias] for the interface alias (oid 1.3.6.1.2.1.31.1.1.1.18), [ifdescr] for the interface description (oid 1.3.6.1.2.1.2.2.1.2), [custom oid] for any custom oid extended by the port number
Toplists
Memory Limit:
5
megabyte
This value limits the size of toplists in RAM memory. If you get a "Not Analyzed" item in a toplist either increase this value or add a filter to the sensor to reduce the data.
OK
Cancel

This section allows to enter the **SNMP Timeout** in seconds (5 to 20 seconds is recommended). As with most other network protocols a sending device (i.e. the computer running PRTG Traffic Grapher) sends out a request to another device and waits to receive a response. This definable value basically allows to configure a delay within which the SNMP response must be received. Should a SNMP response not be received within this specified timeout value, the SNMP sensor will be registered as not being measurable and the sensor will be shown in red to show the error status.

If your PC is a multi-homed system with more than one IP address you may need to specify the IP address that PRTG uses to contact the devices in the **Bind IP** setting.

The checkbox **High Compatibility Mode** should be marked if you get coverage values below 100% although PRTG and the device are running continuously. See next section.

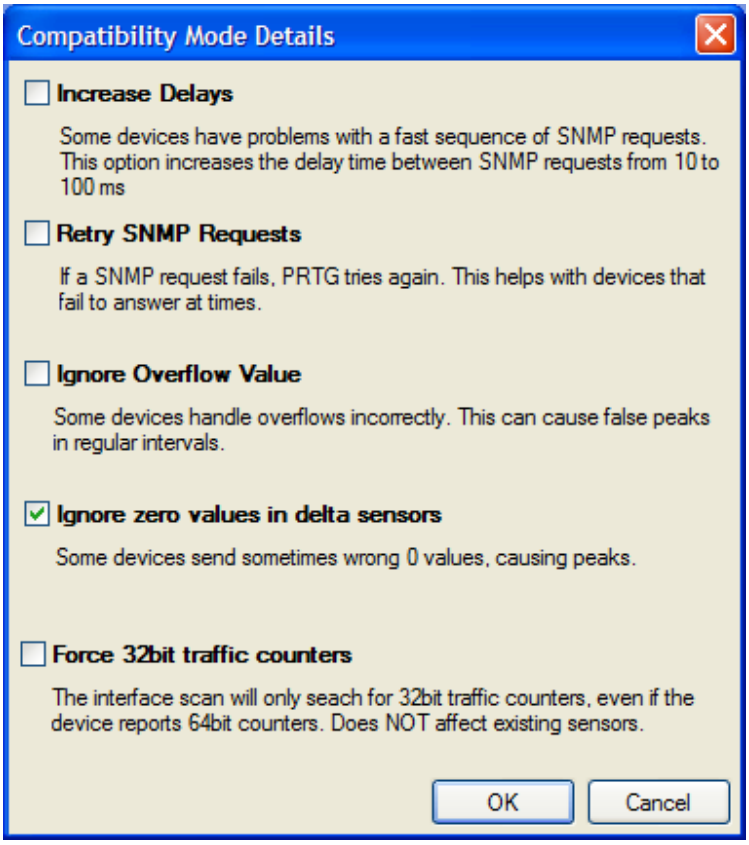
Use the Memory Limit setting to limit the maximum memory that a **toplist** may use in RAM. This is necessary because for high traffic networks e.g. the Top Connections list can grow quite large. The default of 5 MB should be sufficient for most situations.

High Compatibility Mode

It is a feature specifically designed for very sensitive routers and devices, introducing a delay between scanning, allowing these sensitive devices to function properly with PRTG Traffic Grapher.

Note: The High Compatibility Mode may reduce the performance by a small amount!

The High Compatibility Mode also features advanced functionality, accessible via the **Advanced** button:


Compatibility Mode Details
Increase Delays
Some devices have problems with a fast sequence of SNMP requests. This option increases the delay time between SNMP requests from 10 to 100 ms
Retry SNMP Requests
If a SNMP request fails, PRTG tries again. This helps with devices that fail to answer at times.
Ignore Overflow Value
Some devices handle overflows incorrectly. This can cause false peaks in regular intervals.
Ignore zero values in delta sensors
Some devices send sometimes wrong 0 values, causing peaks.
Force 32bit traffic counters
The interface scan will only seach for 32bit traffic counters, even if the device reports 64bit counters. Does NOT affect existing sensors.
OK
Cancel

- **Increase Delays** – In certain cases, devices may have trouble or a security mechanism that denies fast sequences of SNMP requests which PRTG Traffic Grapher sometimes may send. With this checkbox checked, the delay time between SNMP requests is increased from 10 to 500 ms for proper functionality with such devices. This may slow down monitoring for large networks, though.
- **Retry SNMP Requests** – Should an SNMP request fail, checking this checkbox will cause PRTG Traffic Grapher to try the request again. This is useful for devices that fail to respond at times to certain requests.
- **Ignore Overflow Value** – Some devices handle device overflows incorrectly. This can cause false peaks at regular intervals. Checking this checkbox causes PRTG Traffic Grapher to ignore these overflow values and thus eliminate errors caused by this problem.
- **Ignore Zero Values in delta Sensors** – This setting may be necessary for some devices.
- **Force 32bit traffic counters** – There are some devices that offer non-working 64bit counters when scanned initially. With this setting PRTG will always use 32 bit counters which may be more reliable.

Advanced Port Name

With this option it is possible to change the way the traffic sensor names are created by default while a new device is scanned.

The default is: "Port X on #host"

If PRTG finds a interface alias (ifalias) or a description (ifdescr) the text is added after the port number with the alias preferred.

If you want to change this behavior you can activate the "Advanced Port Name" option. Enter any custom text with placeholders for dynamic content in brackets:

- [port] the port number, e.g. 1, 2, or 99 etc.
- [ifalias] the interface alias read from the OID 1.3.6.1.2.1.31.1.1.1.18.x with x as the port number
- [ifdescr] the interface description read from the OID 1.3.6.1.2.1.2.2.1.2.x with x as the port number
- [custom oid] any custom oid e.g. [1.3.6.1.2.1.2.2.1.2] for the same as the [ifdescr] placeholder. The OID is extended with .x for the port number

Example 1: To get a similar result to the default but always use the description field use the following string:

```
Port [port]:[ifdescr]
```

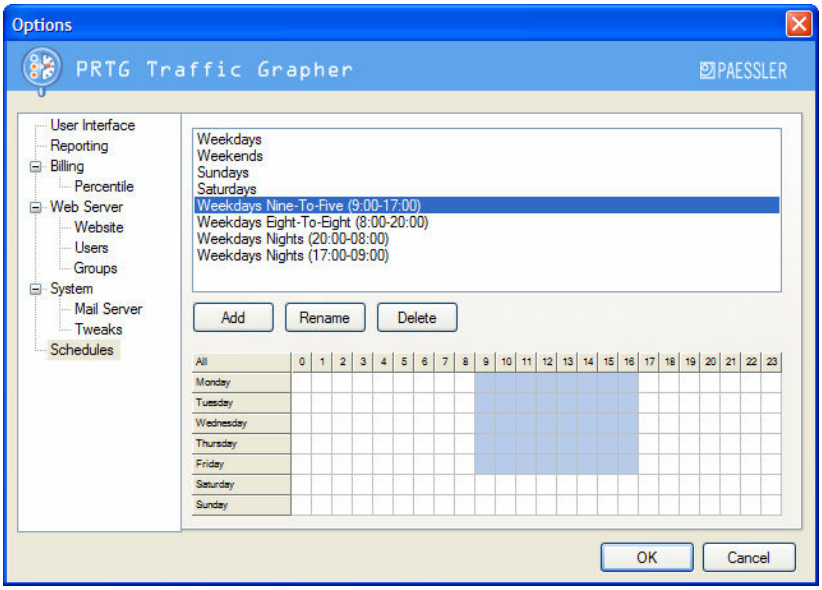
The "on #host" is always automatically added.

Example 2: Cisco routers provide a interface name in the OID 1.3.6.1.4.1.9.2.2.1.1.28 (which stands for iso.org.dod.internet.private.enterprises.cisco.local.linterfaces.lifTable.lifEntry.locIfDescr). You can use this name with this Advanced port name by entering the following string:

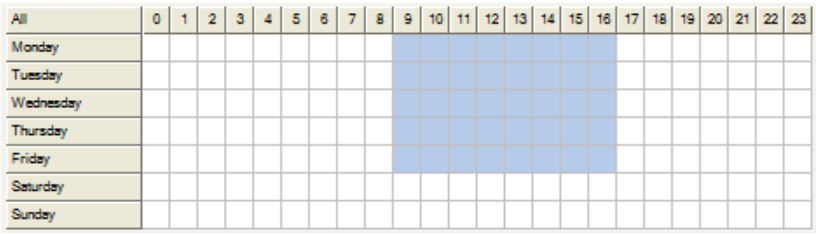
```
Port [port]:[1.3.6.1.4.1.9.2.2.1.1.28]
```

Schedules Settings

Using schedules you can limit the time for monitoring or for notifications. PRTG comes with a number of pre-defined schedules that you can edit, or you can add your own schedules.



Use the **Add**, **Rename** and **Delete** buttons to work with the schedules. A schedule is active of the corresponding square in the graph is marked in blue:



Each square symbolizes one hour. By clicking each square once with the mouse you can activate/deactivate the schedule for this hour.

After you have defined a schedule here you can select it in the sensor settings and the notification settings.

Advanced Usage

Paessler SNMP Helper

Paessler SNMP Helper enables PRTG Traffic Grapher (or its sister product IPCheck Server Monitor) to collect in-depth performance information from Windows servers and workstations. Up to several thousands parameters and performance counters of a PC can be monitored with just a few mouse clicks.

SNMP Helper License Options

There are three different flavors available:

- Freeware Edition: Supports monitoring of memory, disks, network, and processors and comes free with the downloads of PRTG Traffic Grapher and IPCheck Server Monitor
- Pro Edition: Adds more than 2000 performance counters for servers and workstations running Windows 2000, XP or 2003
- Pro Extensions: Are available for in-depth monitoring of MS Exchange Server, MS ISA Server, MS SQL Server and MS Biztalk Server

Fully Integrated Into Paessler's Monitoring Products

Simply install SNMP Helper on Windows 2000, XP or 2003 systems and you can monitor numerous performance counters using PRTG Traffic Grapher and IPCheck Server Monitor - simply by adding new sensors. Both our monitoring products have built-in support for the additional counters. Within a few minutes you will be able to monitor values like "disk writes/s", "DHCP Server Requests/s", "Exchange Server: Messages/s", "SQL Server: Requests/s", and many more.

In our knowledge base at www.paessler.com/support we have compiled a list of recommended performance counters that you can monitor using SNMP Helper.

SNMP Helper Freeware Edition

The Freeware Edition supports about 80 performance counters and is part of PRTG Traffic Grapher and IPCheck Server Monitor. You must install SNMP Helper on the machine(s) you want to monitor. After installation of PRTG or IPCheck you will find the SNMP Helper Freeware setup files in a subfolder. Run this setup on all the systems you want to monitor. Afterwards you can monitor the additional system parameters by simply adding new sensors.

SNMP Helper Pro Edition and its Extensions

The Pro Edition of SNMP Helper offers the ability to monitor more than 2000 counters for Windows 2000, XP, and 2003. With the optional SNMP Helper Extensions you can additionally monitor the following Microsoft Server applications:

- MS Exchange Server: more than 1726 performance counters
- MS SQL Server: more than 511 performance counters
- MS Biztalk Server: 32 performance counters
- MS ISA Server: 149 performance counters

Detailed lists of supported counters are available at www.paessler.com/snmphelper.

To use SNMP Helper Pro you must either purchase a license or you must request a Free 30 Day Trial License. Either way you will receive a license key and the installation files via email. Please install the software on the server that you want to monitor and enter the license key that comes with it. Afterwards you can monitor the additional system parameters by simply adding new sensors to IPCheck and PRTG.

Installing Paessler SNMP Helper

Paessler SNMP Helper is a small library that makes it much easier to access system parameters of Windows machines using SNMP. If the SNMP Helper is installed PRTG Traffic Grapher will be able to read various system parameters from this machine.

SNMP Helper can be used on Windows XP, 2000 and 2003.

You only need to install SNMP Helper on a computer if you want to monitor it! You must install SNMP Helper on each Windows computer you want to monitor using the additional sensors.

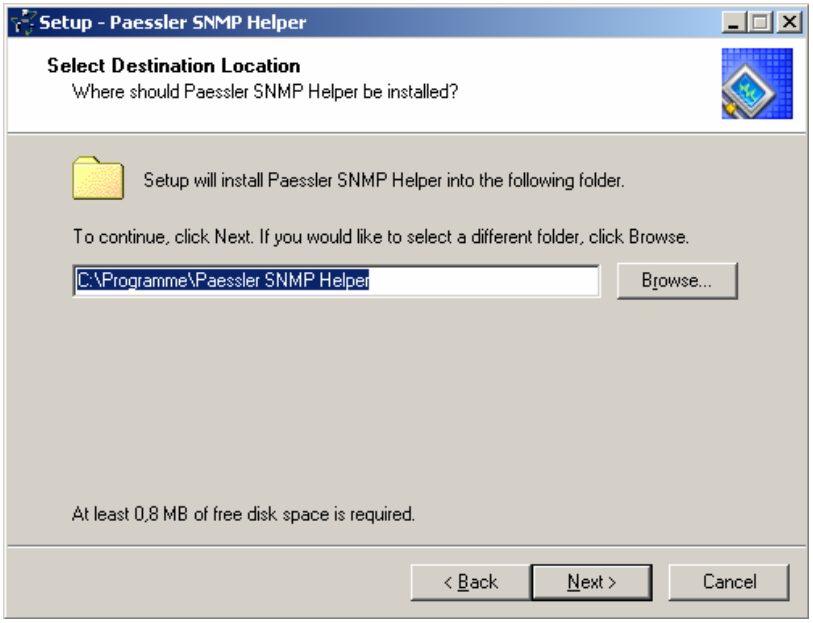
First, make sure to install the Windows SNMP component using the **Add/Remove Software** control from your **Windows Control Panel** (see "Howto: Installing SNMP Service on Windows NT/2000/XP").

In order to install Paessler SNMP Helper, launch the **Paessler SNMP Helper Setup.exe** file located within your PRTG Traffic Grapher installation directory after you have installed PRTG Traffic Grapher.

This will launch the Paessler SNMP Helper Setup Wizard.

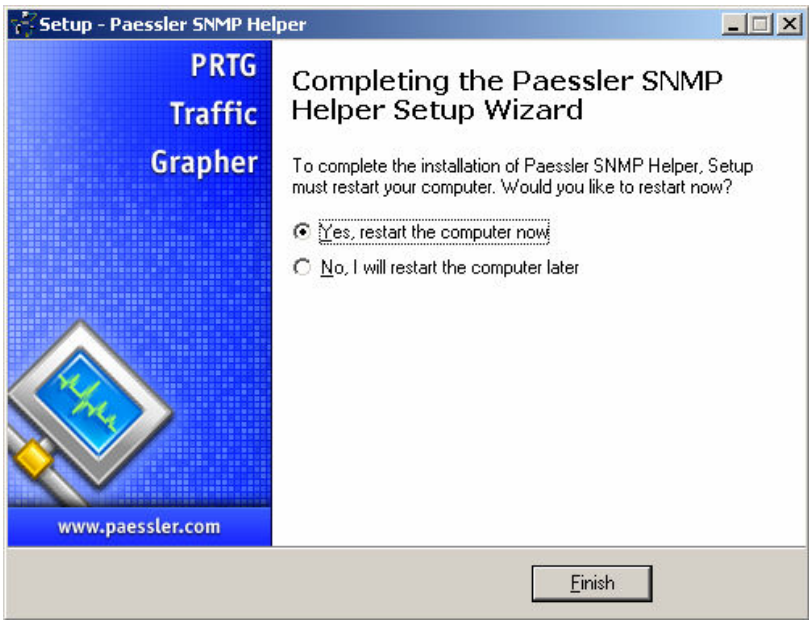
Setup - Paessler SNMP Helper
PRTG
Traffic
Grapher
www.paessler.com
Welcome to the Paessler SNMP Helper Setup Wizard
This will install Paessler SNMP Helper 1.3 on your computer.
It is recommended that you close all other applications before continuing.
Click Next to continue, or Cancel to exit Setup.
Next >
Cancel

Once you have read the information found in the welcome screen click Next to continue installation.


Setup - Paessler SNMP Helper
Select Destination Location
Where should Paessler SNMP Helper be installed?
Setup will install Paessler SNMP Helper into the following folder.
To continue, click Next. If you would like to select a different folder, click Browse.
C:\Programme\Paessler SNMP Helper
Browse...
At least 0,8 MB of free disk space is required.
< Back
Next >
Cancel

From the Select Destination Location window use the Browse button to select a directory in which to install the Paessler SNMP Helper. You can also enter the

destination location directly in the provided box. Once you have chosen your destination location, click on Next to continue.


Setup - Paessler SNMP Helper
PRTG
Traffic
Grapher
Completing the Paessler SNMP Helper Setup Wizard
To complete the installation of Paessler SNMP Helper, Setup must restart your computer. Would you like to restart now?
Yes, restart the computer now
No, I will restart the computer later
www.paessler.com
Finish

Once Paessler SNMP Helper is installed, the program will prompt you that it needs to restart the machine in order to complete the installation process. If you are ready to restart your machine, select this option from the provided menu. Otherwise, select to restart your computer later.

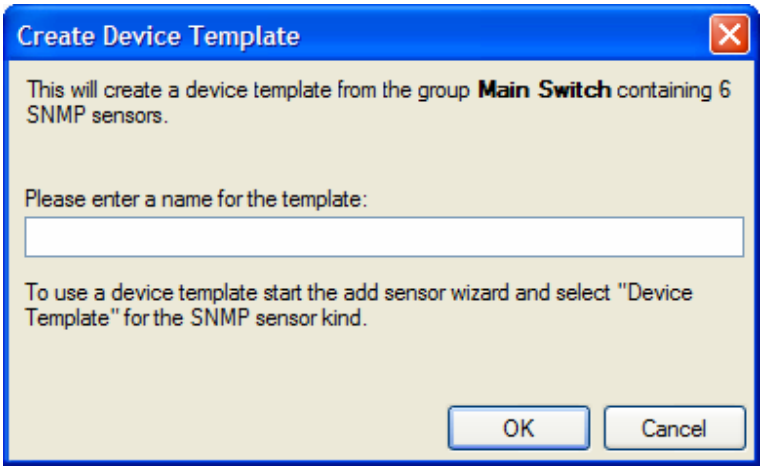
Note: Keep in mind – in order for the Paessler SNMP Helper to work properly, your system has to be restarted. If you opt to restart the machine later you will need to do so before the Paessler SNMP Helper can be fully put into operation.

Working with Device Templates

With device templates you can easily set up a set of sensors for several devices. After creating a set of sensors for the first device you will save the sensor set, which is finally reused to create the same set of sensors for a different device.

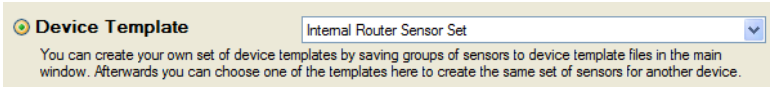
The process works like this: First you create a set of the desired sensors for one device. Move all the sensors into one group.

Right-Click the group name and choose **Create Device Template From Group** (or find this menu item in the **Edit** Menu). You will be asked for a filename:

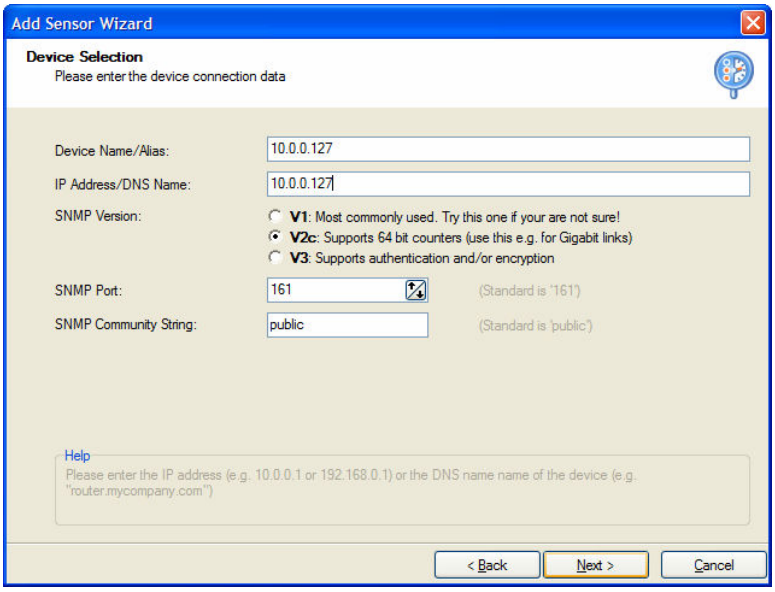

Create Device Template
This will create a device template from the group Main Switch containing 6 SNMP sensors.
Please enter a name for the template:
To use a device template start the add sensor wizard and select "Device Template" for the SNMP sensor kind.
OK
Cancel

Choose a filename and click **OK**.

Now use the **Add Sensor Wizard** to create the same set of sensors for the other devices. Start the wizard, choose **SNMP** sensor and then choose **Device Template** as sensor type.


Device Template
Internal Router Sensor Set
You can create your own set of device templates by saving groups of sensors to device template files in the main window. Afterwards you can choose one of the templates here to create the same set of sensors for another device.

From the dropdown you choose one of your device templates. Click **Next** and enter the IP address of the new device:


Add Sensor Wizard
Device Selection
Please enter the device connection data
Device Name/Alias:
10.0.0.127
IP Address/DNS Name:
10.0.0.127
SNMP Version:
V1: Most commonly used. Try this one if your are not sure!
V2c: Supports 64 bit counters (use this e.g. for Gigabit links)
V3: Supports authentication and/or encryption
SNMP Port:
161
(Standard is '161')
SNMP Community String:
public
(Standard is 'public')
Help
Please enter the IP address (e.g. 10.0.0.1 or 192.168.0.1) or the DNS name name of the device (e.g. "router.mycompany.com")
< Back
Next >
Cancel

Complete the wizard and you will find a new group of sensors for the newly added device.

Initially these sensors are paused to give you a chance to edit the sensors (e.g. to enter a different password, etc.). If you are done with the configuration select the new sensors and click the start button.

Accessing Logfiles

PRTG Traffic Grapher creates two log files. The first is

```
PRTG Traffic Grapher Logfile (application).log
```

and is written while the program runs in GUI mode.

The second file is

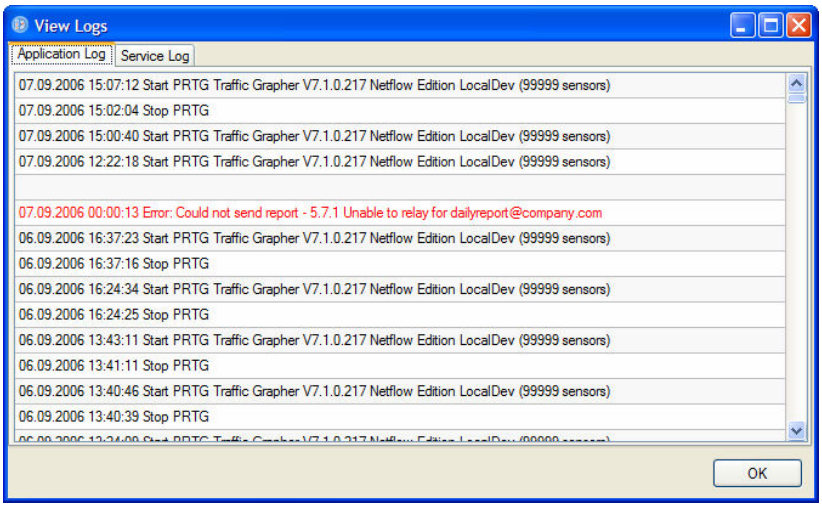
```
"PRTG Traffic Grapher Logfile (service).log"
```

and is written while the program runs as a service

Both files are stored in the folder where the INI file is stored, usually:

```
C:\Documents and Settings\All Users\Documents\PRTG Traffic
Grapher\*.log
```

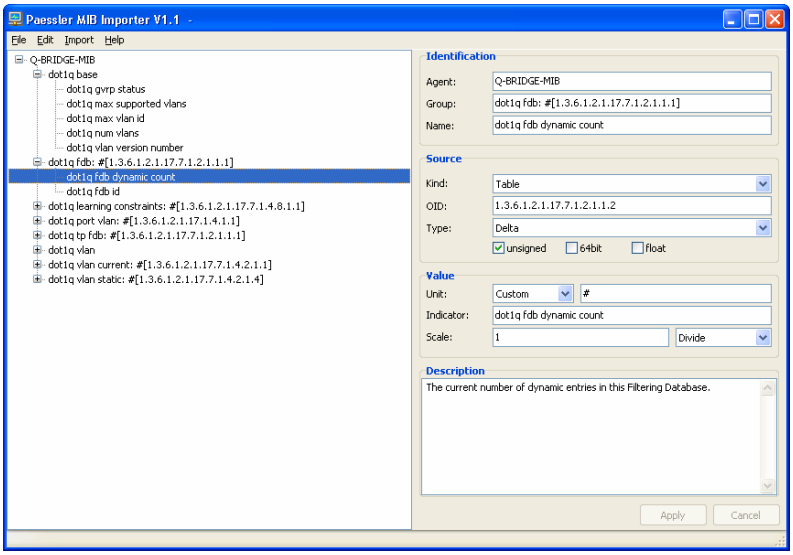
While using PRTG in GUI mode you can view the files using the menu item **Help|View Logfiles**. You can switch between **Application Log** and **Service Log**.


View Logs
Application Log
Service Log
07.09.2006 15:07:12 Start PRTG Traffic Grapher V7.1.0.217 Netflow Edition LocalDev (99999 sensors)
07.09.2006 15:02:04 Stop PRTG
07.09.2006 15:00:40 Start PRTG Traffic Grapher V7.1.0.217 Netflow Edition LocalDev (99999 sensors)
07.09.2006 12:22:18 Start PRTG Traffic Grapher V7.1.0.217 Netflow Edition LocalDev (99999 sensors)
07.09.2006 00:00:13 Error: Could not send report - 5.7.1 Unable to relay for dailyreport@company.com
06.09.2006 16:37:23 Start PRTG Traffic Grapher V7.1.0.217 Netflow Edition LocalDev (99999 sensors)
06.09.2006 16:37:16 Stop PRTG
06.09.2006 16:24:34 Start PRTG Traffic Grapher V7.1.0.217 Netflow Edition LocalDev (99999 sensors)
06.09.2006 16:24:25 Stop PRTG
06.09.2006 13:43:11 Start PRTG Traffic Grapher V7.1.0.217 Netflow Edition LocalDev (99999 sensors)
06.09.2006 13:41:11 Stop PRTG
06.09.2006 13:40:46 Start PRTG Traffic Grapher V7.1.0.217 Netflow Edition LocalDev (99999 sensors)
06.09.2006 13:40:39 Stop PRTG
OK

Importing MIBs using Paessler MIB Importer and Converter

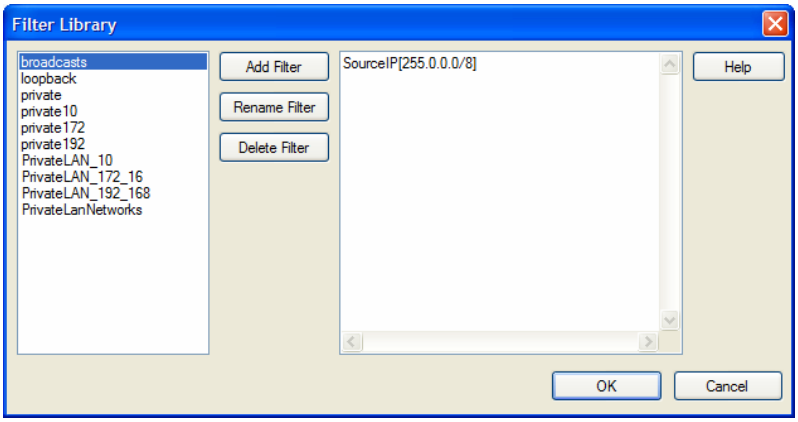
In order to import MIB files from third parties (usually the vendor of a device) into PRTG you must convert the files into OIDLIB files.

The MIB Importer and Converter Tool is available free of charge on the Paessler website at www.paessler.com.

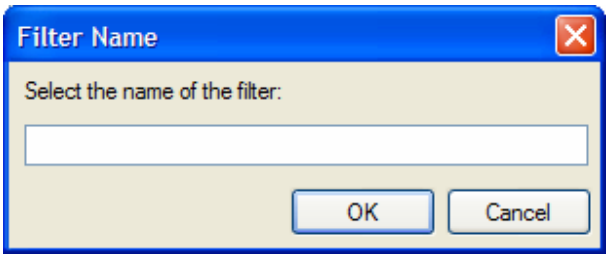


Editing Filter Libraries

You can set up libraries from the **Extras** menu. Select **Filter Library** and the following window will open:

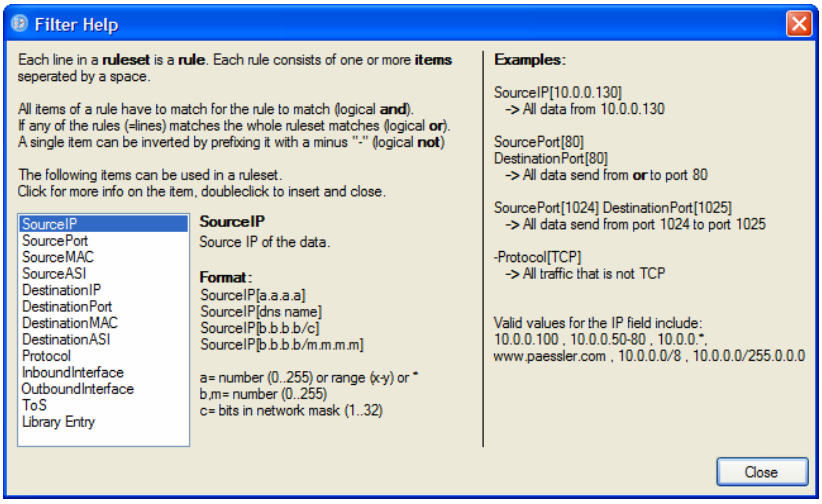


Here you can add and rename filters. When selecting these options, the following window will open:



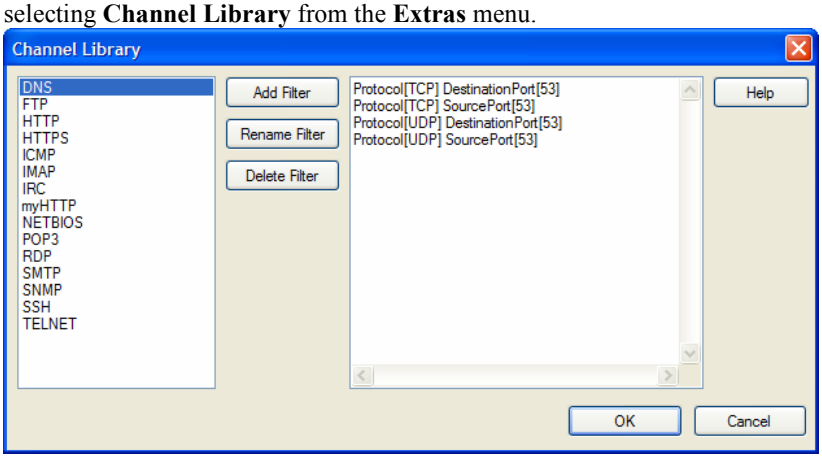
Here you can edit the name of the selected filter.

On the right side you can edit the filter's settings. Please click on **help** for detailed information about the filter language.

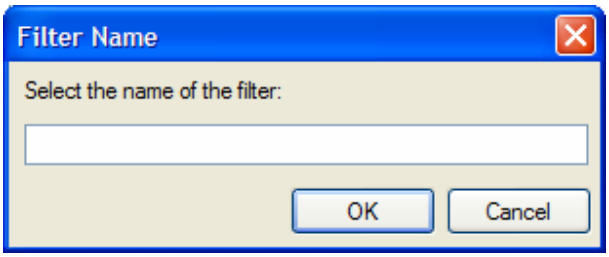

Filter Help
Each line in a ruleset is a rule. Each rule consists of one or more items seperated by a space.
All items of a rule have to match for the rule to match (logical and).
If any of the rules (=lines) matches the whole ruleset matches (logical or).
A single item can be inverted by prefixing it with a minus "-" (logical not)
The following items can be used in a ruleset.
Click for more info on the item, doubleclick to insert and close.
SourceIP
SourcePort
SourceMAC
SourceASI
DestinationIP
DestinationPort
DestinationMAC
DestinationASI
Protocol
InboundInterface
OutboundInterface
ToS
Library Entry
SourceIP
Source IP of the data.
Format:
SourceIP[a.a.a.a]
SourceIP[dns name]
SourceIP[b.b.b.b/c]
SourceIP[b.b.b.b/m.m.m.m]
a= number (0..255) or range (x-y) or *
b,m= number (0..255)
c= bits in network mask (1..32)
Examples:
SourceIP[10.0.0.130]
-> All data from 10.0.0.130
SourcePort[80]
DestinationPort[80]
-> All data send from or to port 80
SourcePort[1024] DestinationPort[1025]
-> All data send from port 1024 to port 1025
-Protocol[TCP]
-> All traffic that is not TCP
Valid values for the IP field include:
10.0.0.100 , 10.0.0.50-80 , 10.0.0.*,
www.paessler.com , 10.0.0.0/8 , 10.0.0.0/255.0.0.0
Close

Editing Channel Libraries

You can edit the library of channels for packet sniffing and NetFlow sensors by selecting **Channel Library** from the **Extras** menu.



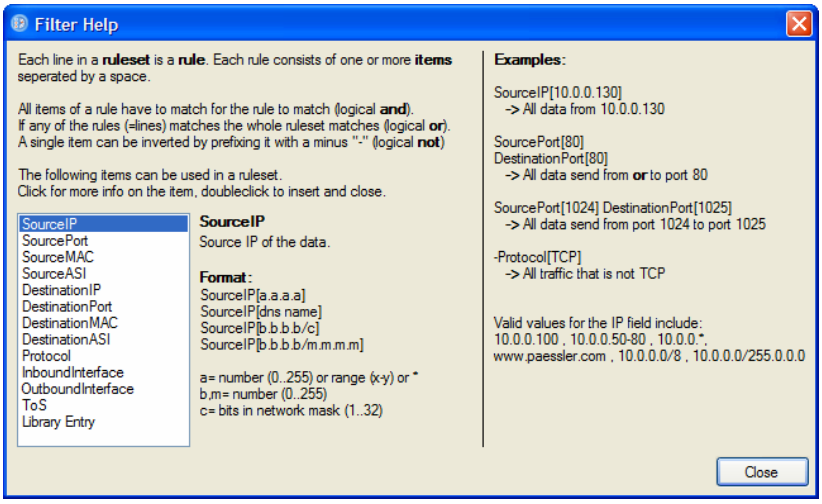
Here you can add and rename filters. These buttons will open the following window:



Enter the desire name (respectively change the desired name) and click **OK** to add / edit the filter.

In order to delete a filter, click on the **Delete Filter** button.

On the right side you can edit the filter's settings. Please click on **help** for detailed information about the filter language.


Filter Help
Each line in a ruleset is a rule. Each rule consists of one or more items seperated by a space.
All items of a rule have to match for the rule to match (logical and).
If any of the rules (=lines) matches the whole ruleset matches (logical or).
A single item can be inverted by prefixing it with a minus "-" (logical not)
The following items can be used in a ruleset.
Click for more info on the item, doubleclick to insert and close.
SourceIP
SourcePort
SourceMAC
SourceASI
DestinationIP
DestinationPort
DestinationMAC
DestinationASI
Protocol
InboundInterface
OutboundInterface
ToS
Library Entry
SourceIP
Source IP of the data.
Format:
SourceIP[a.a.a.a]
SourceIP[dns name]
SourceIP[b.b.b.b/c]
SourceIP[b.b.b.b/m.m.m.m]
a= number (0..255) or range (x-y) or *
b,m= number (0..255)
c= bits in network mask (1..32)
Examples:
SourceIP[10.0.0.130]
-> All data from 10.0.0.130
SourcePort[80]
DestinationPort[80]
-> All data send from or to port 80
SourcePort[1024] DestinationPort[1025]
-> All data send from port 1024 to port 1025
-Protocol[TCP]
-> All traffic that is not TCP
Valid values for the IP field include:
10.0.0.100 , 10.0.0.50-80 , 10.0.0.*,
www.paessler.com , 10.0.0.0/8 , 10.0.0.0/255.0.0.0
Close

Editing the Skin of the Web GUI

In order to edit the look and feel of the Web GUI you must edit the HTML template files in the “webtemplates” subfolder of your installation folder.

Basically there is one main HTML template file PRTG Traffic Grapher builds the main page and all other pages from: global.htm. However, as one moves deeper into the interface, there might be other web templates that need to be edited. All of these, however, are found in the same directory.

When editing this HTML file, please ensure to keep the placeholder structure in a proper manner, as changes to this structure can cause problems when viewing the web-based interface. It is of particular importance not to change the “<#Content>” placeholder, as it is here where the graphs and tables are displayed.

Also, prefer to edit the style sheet at the beginning of the file to achieve the desired layout rather than editing the actual HTML code of the file.

All images used in the web view can also be changed. These files can be found under the appropriate skin (in the webtemplates folder) under the subdirectory “images”.

You can generate additional skins by merely generating a new folder – this will be available as a skin in the drop-down menu of the web interface skin selection. Any name can be used. However, do make sure that all relevant files are to be found in the respective folder.

Note: To edit the HTML files please do not use an HTML editor that actively changes the HTML code (e.g. FrontPage), because very often the code for the placeholders are changed and IPCheck Server Monitor will not work with these files. We recommend to use Windows Notepad or any other plain text editor. Also, always make a backup copy of the original files before changing them!

Restoring Lost Sensor Settings From DAT files

The configuration data for the sensorlist is normally stored in the **.prtg** file. If this file is lost and no backup is available, but the **.dat** files of the historic monitoring database are still there, PRTG Traffic Grapher can recreate the sensorlist from these files.

Important: This only works with files created by Version 5 or later.

Each .dat file contains the sensor configuration from the time the .dat file was created.

The .dat file does not contain user/group settings and the filter/channel libraries. If you restore a packet sniffer or NetFlow sensor make sure that your libraries contain all the required entries.

It is better to use a backup of the .prtg file to restore a configuration (use the automatic backup option to create a copy every day). The .dat import is only intended as last resort to get sensors or data back if only the .dat files are left.

To import a single .dat file click **File|Import|Prtg 5/6 .dat file**. Now select the .dat file. PRTG automatically copies the file to the correct location and adds a group "Imported Sensors" with the restored sensor.

To import multiple .dat files of a single sensor (one .dat file per day). First copy all.dat files to the monitoring database subfolder of your current .prtg file and then import the latest .dat file as described above.

Importing Configuration Files from MRTG

PRTG Traffic Grapher allows you to import MRTG configuration files. In order to do so, use the **File** menu and select the function **Import**. A drop down will open. From here select **MRTG Configuration File** and follow the instructions.

Please note that PRTG only understands a subset of MRTG features, but for standard SNMP sensors most settings should be imported fine.

Appendix

Articles from the Paessler Knowledge Base

This section lists selected articles for PRTG Traffic Grapher from the Paessler Knowledge Base. For additional articles and the most recent and updated information please visit www.paessler.com/support.

How to set up traffic monitoring with PRTG for various infrastructures

This article explains the various options you have to monitor the network traffic that occurs inside LAN or that goes over a shared Internet connection or leased line.

Please see the Knowledge Base at www.paessler.com/support.

Configuration Tips for Cisco Routers and PRTG (NetFlow/SNMP)

This article includes several tips&tricks for your Cisco router configuration when using PRTG Traffic Grapher with SNMP or NetFlow.

Please see the Knowledge Base at www.paessler.com/support.

Netflow 5 Filter Parameters supported by PRTG Traffic Grapher

This article explains the traffic parameters that can be used to filter traffic when NetFlow based bandwidth monitoring is used.

Please see the Knowledge Base at www.paessler.com/support.

Planning large installations of PRTG Traffic Grapher

When planning large installations of PRTG Traffic Grapher with many sensors (>100) or with high traffic (>10 Mbit), there are several parameters to take into account that influence the maximum number of sensors that can be monitored using one single PRTG instance.

Please see the Knowledge Base at www.paessler.com/support.

How PRTG Traffic Grapher stores its data

A short description what files and folders PRTG™ Traffic Grapher uses, where they are located, and what they do.

Please see the Knowledge Base at www.paessler.com/support.

Using live graphs from PRTG in other webpages using static image URLs

If you want to include live graphs from PRTG into your own webpages (e.g. Intranet) that always show the recent traffic pattern you must encode the date in the graphs' URLs in a relative manner. This article explains the parameters of PRTG's graph URLs.

Please see the Knowledge Base at www.paessler.com/support.

How to find out OIDs for PRTG's custom SNMP sensors

Out of the box, PRTG™ Traffic Grapher offers various sensors defined within the various provided libraries. However, sometimes these included libraries do not suffice and it is necessary to access devices by directly providing Object Identifiers (OIDs).

Please see the Knowledge Base at www.paessler.com/support.

Upgrading from PRTG Version 3 to Version 5/6

PRTG Traffic Grapher version 6 can not import historic monitoring data from version 3. You must first upgrade to V4.

Please see the Knowledge Base at www.paessler.com/support.

Why PRTG may stop recording data as soon as the Windows GUI is closed

This article lists reasons why PRTG Traffic Grapher may stop recording data as soon as the WindowsGUI is closed.

Please see the Knowledge Base at www.paessler.com/support.

PRTG service is not started (Event ID 7000/Error 193 in system log)

On some systems the PRTG service is not started automatically and Event 7000 ("Error 193: %1 is not a valid Win32 application.") is written to the system log. This issue may occur if the path of the executable file for the service contains spaces.

Please see the Knowledge Base at www.paessler.com/support.

Automated License Key Installation for PRTG Traffic Grapher

In some situations (e.g. for automated software distribution) it may be desirable to enter and store a license key for PRTG automatically. There are two options to do this.

Please see the Knowledge Base at www.paessler.com/support.

What do the values in the exported CSV log file say?

Please see the Paessler Knowledge Base at www.paessler.com/support.

Howto: Installing SNMP Service on Windows NT/2000/XP

Please note: You need to install the SNMP service only on those Windows machines that you want to monitor using SNMP. It is not necessary to install the SNMP service on the machine you run PRTG Traffic Grapher on if you do not intend to monitor it with PRTG!

The best moment to install the SNMP service is immediately after or as part of the installation of the operating system because there are some applications that check for the availability of the SNMP service to install their own SNMP files. There are some applications (i.e. IIS and MS SQL Server), that will not install SNMP support if the service is not installed (and in some cases, running)!

To install the SNMP on Windows 2000/XP, perform the following (note the process is very similar on Windows NT 4):

- Click on **Start | Settings | Control Panel**.

- Double-click on **Add/Remove Programs**.
- Click on **Add/Remove Windows Components**.
- Click on **Management and Monitoring Tools** and click on **Details**.
- Check **Simple Network Management Protocol** and click OK.
- Click on **Next** and let the install process complete.
- Double-click on **Administrative Tools** (inside Control Panel).
- Double-click on **Computer Management**.
- Expand the **Services and Applications** tree on the left frame.
- Click on **Services** on the left frame.
- Locate **SNMP Service** in the right frame and double-click on it.
- On the **General** tab, select **Automatic** for **Startup Type**.
- On the **Security** tab you can leave the default community name "public" or choose your own (which is more secure). To choose your own , click on **Add...** for Accepted community names, leave **Community Rights** to Read-Only and pick a secure **Community Name**. Click on **OK**. Remove the "public" entry
- On the **Security** tab in the lower half you can choose which IP addresses are allowed to access the SNMP service. You must at least choose the IP address of the machine running PRTG!
- On the **Agent** tab fill out all edit fields and enable all check boxes to make all SNMP values available.
- For added flexibility we recommend to install Paessler SNMP Helper that comes included with the PRTG Traffic Grapher files (see Paessler SNMP Helper).

The following links may also be helpful with the setup:

- Search for SNMP in the Microsoft Knowledge Base: http://search.microsoft.com/search/results.aspx?qu=snmp
- Windows 2000 Server Resource Kit: SNMP Simple Network Management Protocol http://www.microsoft.com/resources/documentation/windows/2000/server/reskit/en-us/tcpip/part3/tcpch10.mspx
- HOW TO: Configure Security for a Simple Network Management Protocol Service in Windows 2000: http://support.microsoft.com/default.aspx?scid=KB;EN-US;q315154&

Howto: Installing SNMP on Linux

Suitable SNMP software and instructions should be available from the vendor of your Linux distribution.

SNMPD from the Net-SNMP project is very commonly used, see: net-snmp.sourceforge.net/

There is a good tutorial that explains the installation of the NET-SNMP deamon on a Debian Linux system on the DebianHelp website: www.debianhelp.co.uk/snmp.htm

After installing and configuring this daemon you should be able to monitor vital system data (e.g. the CPU load) using PRTG Traffic Grapher. Simply create a new sensor, choose "SNMP Library Sensor" and select the "Basic Linux Library" from the list of available libraries.

Howto: Troubleshooting the device setup when using SNMP

If you are using a SNMP Sensor the SNMP protocol (Simple Network Management Protocol) must be installed and enabled on your device.

Please go through the following checklist:

- Is SNMP installed and enabled on the device? (see configuration of the device)
- Does your machine running PRTG Traffic Grapher have access to the SNMP connection on that device? (see device's security settings)
- Double check the "SNMP Community String" (this value is case sensitive)
- Check the SNMP Port (usually it is 161)
- Firewall issues: If the device and the monitoring machine are on two different sides of a firewall make sure that UDP access to port 161 (SNMP) is allowed and you will also need the return path open. SNMP uses UDP not TCP, so SNMP requires the use of UDP ports >1023 to the PRTG client side so that the results can be sent back from the device to the machine running PRTG.

If you have verified the issues above also check the SNMP Tweaks in the **Extras|Options** dialog.

Support and License

Support

Please visit http://www.paessler.com/support for support options.

Copyright

Copyright for this software © 1998-2007 Paessler AG

Paessler AG
Hornschuchpromenade 7
D-90762 Fürth
Germany

E-Mail: info@paessler.com
Company Homepage: http://www.paessler.com

PRTG® and Paessler® are registered trademarks of Paessler.

Consulting and Custom Software

Paessler offers consulting and development of custom software. Please inquire via email to sales@paessler.com.

License/Usage Terms

PLEASE READ THESE GENERAL TERMS AND CONDITIONS CAREFULLY.

§ 1 TERRITORY

These General Terms and Conditions govern the use and maintenance of the Paessler Software for customers who use the software outside the Federal Republic of Germany. The use of the Paessler Software in the territory of the Federal Republic of Germany is governed by the "Allgemeinen Lizenzbedingungen der Paessler AG".

§ 2 DEFINITIONS

Site: Defined and/or restricted area (e.g. campus, premises) of which the diameter does not exceed 6,21 miles (10 kilometers), and which is used exclusively by the customer;

Customer: Contract partner who licensed the Paessler Software;

User: Person working with the software.

§ 3 PRE-CONDITION

PAESSLER AG IS WILLING TO LICENSE THE PAESSLER SOFTWARE TO THE CUSTOMER ONLY ON THE CONDITION THAT THE CUSTOMER ACCEPTS ALL OF THE TERMS CONTAINED IN THIS AGREEMENT.

§ 4 ASSIGNMENT

BY DOWNLOADING OR INSTALLING THIS SOFTWARE, THE CUSTOMER ACCEPTS THE TERMS OF THESE GENERAL TERMS AND CONDITIONS AND INDICATES THE ACCEPTANCE THEROF BY SELECTING THE "ACCEPT" BUTTON AT THE BOTTOM OF THESE GENERAL TERMS AND CONDITIONS. IF THE CUSTOMER IS NOT WILLING TO BE BOUND BY ALL THE TERMS, THE CUSTOMER SELECTS THE "DECLINE" BUTTON AT THE BOTTOM OF THE AGREEMENT AND THE DOWNLOAD OR INSTALL PROCESS WILL BE INTERRUPTED.

§ 5 LICENCES

Paessler grants to the customer a non-exclusive license to use the Paessler Software in object code form as described in these General Terms and Conditions.

1. “Commercial-Edition”

The “Commercial-Edition-Software” is designed for the exclusive use by the customer. For the grant of license a fee has to be paid.

The „Commercial-Edition“-License is non-transferable. Any attempt to share or transfer a licence without the consent of Paessler shall be a violation of this license agreement and international copyright laws, and will result in the forfeit of all benefits and rights as a user.

A. Single- and Multi-user license

The customer purchases a certain number of licences according to the confirmation of order. The customer is only allowed to install and use the maximum number of purchased licences simultaneously. This means the customer may only use the modules contained within the software for which the customer has paid a license fee and for which the customer has received a product authorization key from Paessler.

If the number of licenses allowed to be use simultaneously is exceeded, Paessler has to be informed and the exceeded number of installations have to be prevented through suitable means.

If the exceeded number of installations can not be prevented by organizational oder technical means, the customer is obliged to purchase the relevant number of licences.

B. Site- License

Paessler grants the customer the right and license to install and use the software on multiple computers for one or more users.

This license, however, is restricted to the use within one location (site). In the case of the software being used in other locations than those agreed upon, the customer is obliged to pay the license fee due for the location-license as a compensation.

C.Verification

The customer grants Paessler or its independent accountants the right to examine the customer´s books, records, and accounts during the customer's normal business hours to verify compliance with the above provisions.

2. “Trial-Edition”

"Trial Edition" means a free-of-charge-version of the software to be used only to review, demonstrate, and evaluate the software. The Trial-Edition may have limited features, and /or will cease operating after a pre-determined amount of time, due to an internal mechanism within the Trial-Edition.

No maintenance is available for the Trial-Edition.

The software may be installed on multiple computers for private and commercial use.

The software may be transferred to third parties (e.g. on homepages or ftp-servers) as long as the program remains unchanged and is offered free of charge. A chargeable transfer of the “Trial-Edition” (chargeable download, CD in Magazins) requires previous written permission by Paessler.

§ 6 RESTRICTIONS

Software under these General Terms and Conditions is confidential and copyrighted. The title to the software and all associated intellectual property rights are retained by Paessler.

The customer may not modify, decompile, or reverse engineer said software.

The customer may make archival copies of the software.

§ 7 MAINTENANCE

Object of the Maintenance Agreement is the maintenance of the “Commercial-Edition-Software” according to the confirmation of order.

1. Scope of Maintenance

The customer is granted the opportunity of downloading the current version of the purchased Commercial-Edition-Software and requesting a license-key anew for the duration of the Maintenance Agreement.

The customer will receive support for the duration of the Maintenance Agreement.

2. Duration

The Maintenance Agreement has a duration of 12 months and may be prolonged.

3. Beginning

The Maintenance Agreement starts with the sending of the affirmation of contract. The affirmation includes the download-link and the licence-key of the software.

4. Prolongation

Prolongation may only take place until the end of the duration of the Maintenance Agreement.

§ 8 PRICE

All levies, dues, taxes, duties, and other charges shall be borne by the customer.

§ 9 PAYMENT

The payment to be made by the customer is in any event due at the time delivery of the software is effected. The due time for payment arises without any further precondition.

The payment to be made by the customer is to be transferred as stated on the invoice to the banking account of Paessler without deduction and free of expenses and costs for Paessler.

In the event of delay in payment the customer will pay to Paessler - without prejudice to compensation for further losses — the costs of judicial and extra judicial means and proceedings as well as interest at the rate of 5 % over the base interest rate of the European Central Bank.

§ 10 LIMITATIONS FOR CUSTOMERS IN THE UNITED STATES AND UNITED STATES TERRITORY

1. LIMITED WARRANTY

Paessler warrants that for a period of ninety (90) days from the date of download the software files will be free of defects as regards the product under normal use. Except for the foregoing, software is provided "AS IS". The customer´s exclusive remedy and Paessler's entire liability under this limited warranty will be at Paessler's option to replace software media or refund the fee paid for the software. Any implied warranties on the software are limited to 90 days.

2. DISCLAIMER OF WARRANTY

UNLESS SPECIFIED IN THESE GENERAL TERMS AND CONDITIONS, ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF

MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT ARE DISCLAIMED, EXCEPT TO THE EXTENT ALLOWED BY APPLICABLE LAW.

3. LIMITATION OF LIABILITY

IN NO EVENT WILL Paessler BE LIABLE FOR ANY LOST OF REVENUE, PROFIT OR DATA, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL OR PUNITIVE DAMAGES, HOWEVER CAUSED REGARDLESS OF THE THEORY OF LIABILITY, ARISING OUT OF OR RELATED TO THE USE OF OR INABILITY TO USE SOFTWARE, EVEN IF Paessler HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, EXCEPT TO THE EXTENT ALLOWED BY APPLICABLE LAW.

In no event shall Paessler's liability to the customer, whether in contract, tort (including negligence), or otherwise, exceed the price paid by the customer. The foregoing limitations shall apply even if the above-stated warranty fails its essential purpose.

If the Terms above are not applicable to the customer the following Limitations apply.

§ 11 INTERNATIONAL LIMITATIONS

1. Conformity of the Software

The software does not conform with these General Terms and Conditions if at the time the risk passes it is clearly different to the specifications, or in the absence of specifications, the software is not fit for the usual purpose.

Paessler is particularly not liable for the software being fit for a particular purpose to which the customer intends to put it or for the software´s compliance with the legal requirements existing outside the Federal Republic of Germany.

2. Examination and Notice of Lack of Conformity

The customer must examine the software as required by law.

The customer shall give notice of any lack of conformity to Paessler as required by law, in any event directly and in writing and by the quickest possible means by which delivery is guaranteed (e.g. by telefax).

3. Consequence of Delivering non-conforming Software

Following due notice of lack of conformity, the customer can rely on the remedies provided for by the UN Sales Convention in regard to the terms laid down in these General Terms and Conditions. In the event of notice not having been properly given, the customer may only rely on the remedies if Paessler has fraudulently concealed the lack of conformity.

The customer is entitled to demand delivery of substitute software or repair or reduction of the purchase price as set forth in and in accordance with the terms of the UN Sales Convention.

Irrespective of the customer's remedies, Paessler is entitled to repair non-conforming software or to supply substitute software.

4. Third Party Claims and Product Liability

A. Third Party Claims

Without prejudice of further legal requirements, third parties' rights or claims founded on industrial or other intellectual property only found a defect in title to the extent that the industrial and intellectual property is registered and made public in the Federal Republic of Germany.

The customer's claims for defects in title including those founded on industrial or intellectual property will be time-barred according to the same rules as the claims for delivery of non-conforming software.

Third parties not involved in the conclusion of contract based on these General Terms and Conditions in particular those purchasing from the customer, are not entitled to rely on any remedy provided for in this General Terms and Conditions or to raise claims against Paessler, founded on delivery of non-conforming software or defect in title.

B. Product Liability

Without prejudice to Paessler's continuing legal rights and waving any defense of limitation the customer will indemnify Paessler without limit against any and all claims of third parties which are brought against Paessler on the ground of product liability, to the extent that the claim is based on circumstances which are caused after risk passed by the customer.

5. Damages

A. Obligation to Pay Damages

Paessler is only obliged to pay damages pursuant to these General Terms and Conditions if it deliberately or in circumstances amounting to gross negligence breaches obligations owed to the customer. This limitation does not apply if Paessler commits a fundamental breach of its obligations.

Without prejudice to its continuing legal rights, Paessler is not liable for a failure to perform any of its obligations if the failure is due to impediments which occur, e.g. as a consequence of natural or political events, acts of state, industrial disputes, sabotage, accidents, or similar circumstances and which can not be controlled by Paessler through reasonable means.

The customer is required in the first instance to rely on other remedies and can only claim damages in the event of a continuing deficiency.

B. Amount of Damages

In the event of contractual or extra contractual liability Paessler will compensate the loss of the customer to the extent that it was foreseeable to Paessler at the time of the formation of the General Terms and Conditions.

§ 12 MISCELLANEOUS

1.Set off, Suspending Performance

Legal Rights of the customer to set-off against claims of Paessler for payment are excluded, except where the corresponding claim of the customer has either been finally judicially determined or recognized by Paessler in writing.

2. Place of Performance

The place of performance and payment for all obligations arising from the legal relationship between Paessler and the customer is Fürth (Germany).

3. Applicable Law

The legal relationship with the customer is governed by the United Nations Convention of 11 April 1980 on General Terms and Conditions for the International Sale of Goods (UN Sales Convention) in the English version.

Outside the application of the UN Sales Convention, the contractual and non-contractual legal relationship between the parties is governed by the non-uniform German law, namely by the BGB/HGB (German civil and commercial code).

4. Jurisdiction

The parties submit for all contractual and extra-contractual disputes arising from these General Terms and Conditions to the local and international exclusive jurisdiction of the courts having jurisdiction for Fürth (Germany).

5. Communication

All communications, declarations, notices, etc. are to be drawn up exclusively in the German or English language. Communications by means of e-mail or fax need to fulfill the requirement of being in writing.

6. Severability

If provisions of these General Terms and Conditions should be or become partly or wholy void, the remaining conditions continue to apply.

Please contact sales@paessler.com for information on other available license models and volume discounts.

Acknowledgements

Build using Indy Internet Direct - http://www.indyproject.org/.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

Uses the net-SNMP library, see “netsnmp-license.txt”

Uses the DelphiZip library distributed under the GNU LESSER GENERAL PUBLIC LICENSE, http://www.delphizip.net/.

Uses the Info.Zip library, license info in the provided info-zip-license.txt.